1817-4874-1-SM

by Naufal Bahresy

Submission date: 10-Jun-2020 04:36AM (UTC+0700)
Submission ID: 1340921910
File name: 1817-4874-1-SM.docx (312.17K)
Word count: 3663
Character count: 25677

JIKO (Jurnal Informatika dan Ilmu Komputer) Akreditasi KEMENRISTEKDIKTI, No.36/E/KPT/2019
Vol. x, No. x, April 2019, hlm. x-x ISSN: 2355-7699
DOI: 10.33387/jiko e-ISSN: 2528-6579

ANALISIS HALAMAN DARKWEB UNTUK MENDUKUNG INVESTIGASI KEJAHATAN

Muhammad Naufal Bahreisy[1], Ridho Rahmadi[2], Yudi Prayudi[3]

[1] Program Studi Magister Teknik Informatika
[2]Universitas Islam Indonesia1
[3]Universitas Islam Indonesia2
Email: [1]16917113@students.uii.ac.id, [2]ridho.rahmadi.ac.id, [3]prayudi @uii.ac.id

(Naskah masuk: dd mmm yyyy, diterima untuk diterbitkan: dd mmm yyyy)

Abstrak

Dark Web merupakan konten online yang terenkripsi dan hanya dapat di akses menggunakan jaringan khusus seperti *TOR (The Onion Router)*. Saat ini perkembangan konten *online* menjadi perhatian serius karena pertumbuhan bagi kegiatan dan layanan terlarang seperti penjualan barang *illegal*, narkoba dan pornografi anak. Kejahatan komputer dalam dunia internet mendorong banyaknya pertumbuhan transaksi jual beli barang-barang *illegal* yang dijual dipasar gelap, transaksi yang menguntukan namun *illegal* menarik perhatian. *Dark Web* merupakan salah satu media yang digunakan. *Dark Web* merupakan istilah web yang dikategorikan sebagai *Deep Web* yang berdomain .onion yang tidak dapat ditemukan di mesin pencarian seperti *google*, *yahoo* dan *bing*. Analisis halaman-halaman *Dark Web* dalam mendukung investigasi kejahatan diusulkan sebagai solusi untuk memecahkan masalah tersebut. Konsep ini berupa analisis halaman-halaman *Dark Web* yang diharapkan mendukung dalam investigasi kejahatan. Dalam penelitian ini akan dilakukan analisis dari hasil capturing halaman-halaman *Dark Web*. Berdasarkan hasil analsis kemudian diklasifikasikan berdasarkan kategori dengan merefleksikan pada grafik sesuai klasifikasi. pada penelitian ini didapatkan informasi yang penting untuk melakukan analisis halaman-halaman *Dark Web*, seperti informasi tentang jumlah frekuensi kata tertinggi dan vendor yang berkaitan dengan hal tersebut..

Kata kunci: *Dark Web; illegal; TOR (The Onion Router)*

THE ANALYSIS OF THE DARK WEB PAGES IN SUPPORT CRIME INVESTIGATION

Abstract

Dark Web is an encrypted online content that can only be accessed using a dedicated network such as TOR (The Onion Router). Nowadays the development of online content is a serious concern because of growth for illegal activities and services such as the sale of illegal goods, drugs and child pornography. Computer crimes in the Internet world encourages the growing number of trade transactions for illegal goods that are sold in dark markets, transactions that are illegal but attract attention. Dark Web is one of the media used. Dark Web is a web term that is categorized as a Deep Web that has domain .onion that cannot be found in search engines such as Google, Yahoo and Bing. The analysis of the Dark Web pages in support crime investigation is proposed as a solution to solve the problem. This concept constitutes the analysis of Dark Web pages that are expected to support the investigation of crimes. In this study will be conducted analysis of the results capturing the pages of Dark Web. Based on the analysis results are then classified by category by reflecting on the chart according to classification. In this study obtained information that is important for conducting the analysis of Dark Web pages, such as information about the highest number of word frequency and vendor related to it.

Keywords: *Dark Web; illegal; TOR (The Onion Router)*

1. PENDAHULUAN

Lahirnya internet dengan membuat penggunanya dapat berkomunikasi secara geografis berjauhan, namun seolah-olah mereka berada berdekatan. Kehadiran internet memberikan banyak kemudahan bagi penggunanya muali dari mudahnya bertukar informasi sampai memanfaatkan, sebagai sarana komunikasi untuk memperdagangkan barang atau jasa yang melanggar hukum, munculnya beberapa kasus

cybercrime di Indonesia, seperti *hacking* beberapa situs, pencurian kartu kredit, pornografi, penjualan barang illegal, menyadap transmisi data orang lain, misalnya *email* dan memanipulasi data dikomputer yang telah disisipkan menggunakan perintah yang tidak dikehendaki.

Ranah dunia maya begitu dinamis dan memunculkan ragam area yang menarik untuk dikaji lebih dalam. Word Wide Web yang lebih akrab ("*Clear Web*") relatif mudah untuk dilalui, menggunakan *browser google, yahoo* dan *bing* web. Namun sesungguhnya *Word Wide Web* hanya menyumbang Sebagian dari lalu lintas internet, sementara konten diinternet tidak terindeks di sebut sebagai *Deep Web* [1]. Bagian yang tidak terindeks dan sengaja disembunyikan dan tidak dapat diakses oleh browser standar disebut sebagai *Dark Web* [2]Untuk mengakses *Deep web* yang kita perlukan ilmu tentang mesin pencarian seperti *intute, DeepPeep, Scirus* dan *WWW Virtual Library*.

Dark web yang merupakan bagian dari *Deep web* yang tidak dapat ditemukan di mesin pencarian seperti *google, yahoo* dan *bing*. Dalam hal ini ada beberapa situs jual beli narkotika, pornografi, peretasan, situs kekerasan. Hampir semua dari situs *Deep Web* yang dikenal dengan dot onion namun situs berdomain *onion* tersebut bukan *Deep Web* secara keseluruhan *dot onion* merupakan sebagian kecil dari *Deep Web* yang biasa disebut *Dark Web* atau sisi gelap internet. *Deep Web* merupakan bagian dari internet tetapi tidak termasuk ke bagian internet yang dapat diakses mesin pencarian seperti *google.com*.

Sifat terarang dari bisnis yang dilakukan pada pada *Dark Web* banyak pengguna memutuskan untuk mengenkripsi komunikasi mereka. Pesan yang paling umum program enkripsi yang digunakan adalah *PGP (pretty good privacy)* [3].

Berdasarkan penelitian yang dilakukan oleh *Wilson Center* mengenai *The Deep Web and The Darknet* pada tahun 2015 dikatakan bahwa *Google* saat ini sebagai mesin pencarian terbesar hanya mengindeks 4-16 persen dari *Surface web*. Sedangkan *Deep web* lebih besar 400-500 kali dari *Surface web*, dan menurut penelitian yang telah dilakukan [4]bahwa *Dark Web* terbukti sebagai web yang memfasilitasi penjualan barang-barang terlarang seperti *"drugs"*, situs penyewaan pembunuhan dan lain sebagianya. .

Dark Web merupakan istilah umum bagi web dimana orang dapat berinteraksi secara bebas tanpa khawatir atas pengawasan pemerintah. Situs-situs yang dikategorikan dalam *Dark Web* dijaga oleh mekanisme enkripsi yang memungkinkan pengguna menggunjungi situs secara anonim. Pada *Dark Web* alamat situs yang dapat dikunjungi tidak diketik secara gambalang seperti *googl.com* melaikan mengetik alamat URL yang lebih Panjang dan kompleks sebagia contoh, apabila pengguna ingin mengkses *Dark web* pengguna harus menggunakan *browser Tor* sebagai contoh alamat situs *Dark web* yaitu pada web *Hidden Wiki* seperti *url* alamat kpvz7ki2v5agwt35.onion[5].

Berdasarkan pemaparan dari di atas terkait *Dark Web*, dapat diketahui bahwa banyak situs *Dark Web* terdapat tindak kejahatan. Sulitnya menganalsisi *Dark Web* sehingga diperlukan analsisi data pada halaman-halaman *Dark Web* dalam mendukung investigasi kejahatan. Oleh sebab itu penulis berasumsi bahwa menganalisa halaman-halaman pada *Dark Web* diharapkan mendapatkan informasi dalam mendukung investigasi kejahatan

2. LANDASAN TEORI

2.1 Bukti Digital

Keberadaan barang bukti digital menjadi barang bukti penting dalam sebuah kasus kejahatan komputer. Bukti digital dimulai sebagai data elektronik, baik dalam bentuk transaksi, dokumen, atau beberapa jenis media seperti rekaman audio atau video[6]. Transaksi termasuk transaksi keuangan yang dibuat selama proses pembelian, membayar tagihan, menarik uang tunai, dan bahkan menulis cek. Walaupun menulis cek mungkin tampak sebagai metode kuno yang tidak bersifat digital atau elektronik, pemrosesan cek tertulis elektronik dan disimpan di bank atau perusahaan kartu kredit. Hampir setiap jenis transaksi hari ini akhirnya didigitalkan di beberapa titik dan menjadi barang bukti digital: kunjungan dokter, proyek konstruksi, mengisi resep, mendaftarkan anak di tempat penitipan anak, dan bahkan membawa hewan peliharaan untuk mendapatkan suntikan rabies.

2.2 Dark Web

Jika menganggap web sebagai lautan data, sebagian besar dari kita berinteraksi dengen *Surface Web* yang tergolong mudah ditelusuri dan terindeks di mensin pecari yang bisa digunakan seperti *google, yahoo* dan *bing*. Berbeda dengan *Dark Web* yang biasa digambarkan segmen dari web yang mendalam digambarkan sebagai web tersembunyi yang menyatakan bahwa pengguna web tidak dapat dengan mudah mengakses *Dark Web* dengan harapan mereka dapat berbagi informasi dan file dengan sedikit resiko terdeteksi[7]. *Dark Web* merupakan konten *Word Wide Web* yang berada di sisi lain dari internet yang tidak bisa diakses melalui mesin pencari yang biasa digunakan pada umumnya. *Dark Web* dalam paradigma realitas *internet* diibaratakan seperti lingkungan yang buruk didunia nyata, yang mana kecenderungan perilaku kejahatan siber lebih banyak seperti halnya dunia nyata, ada kemungkinan orang baik berada dilingkungan buruk[5]. Namun kecenderungan kearah aktivitas *illegal* lebih besar. *Dark Web* bisa juga disebut *Darknet* bagian dari *Deep Web* yang hanya bisa diakses menggunakan sesuatu

yang khusus untuk dapat mengksesnya, mislanya menggunakan *proxy* atau autentikasi khusus untuk dapat mengakses *Dark Web*, URL situs yang berdomain ".onion" tersebar diantara server seluruh dunia dan tidak terpusat disuatu tempat. *Dark Web* merupakan bagian kecil dari *Deep Web* yang isinya disembunyikan untuk tujuan tertentu. *Dark Web* meminta alat khusus untuk dapat mengakses kontennya dan memerlukan tingkat enkripsi tertinggi. *Dark Web* menampung aktivitas criminal dan sering digunkan oleh jurnalis dan orang lain untuk bertukan informasi sensitif [8].

Deep Web dan *Darknet* tidak memiliki lokasi khusus akan tetapi terdistribusikan di seluruh internet dan berbagi satu kesamaan yaitu tersembunyi dari mesin pencari dari pengguna internet biasa[9]. Orang dapat mencari situs *darknet* hanya dengan mengetik *.onion* atau *.onion* sites atau menemukan website yang sama seperti *Tor Hidden Wiki, Onion.city* dan *DNStats*. Pengguna memerlukan *software* khusus untuk mengaksesnya. Mengkategorikan teknik *forensik* dalam penelitiannya untuk *darknet forensic* menjadi dua kategori yaitu *TOR forensics* dan *Bitcoin forensics*.

Menurut penelitiaan yang dilakukan oleh[9] menjelaskan beberapa kategori level dalam *Deep web* mulai dari 1 samapi dengan level 5 penjelasan kategori level dalam *Deep web* sebagai berikut .

1. **Level 1**dalah bagian web biasa yang paling umum dan dapat memahaminya secara umum. Akan tetapi bukan untuk public di web
2. **Level 2** adalah bagian web yang dikenal sebagai *surface web,* layanan seperti Reddit, Digg, dan email termasuk didalamnya. Konten-konten pendukung sosial lainnya dapat ditemukan di tingkat ini karena pada dasarnya merupakan platform komunikasi dan mencapainya tidak sulit.
3. **Level 3** disebut *Bargie web* yaitu layanan selain *WWW* atau *Web* yang dapat dikategorikan dalam web ini.seperti *newsgroups, Google locked, FTP site, honeypots* dan lain sebagianya seperti 4Chan. Situs ini dikategorikan mudah dijangkau.
4. **Level 4** dikenal sebagai *charter web* atau *Deep web*. *Hacker groups*, aktifitas media terlarang dan lain sebagianya, situs ini biada disebut dengan web dalam yang dengan mesin pencariaan biasa tidak dapat menjangkaunya.
5. **Level 5** dilevel ini segalanya sedikit menyeramkan. Tingkat ini dikenal sebagai *Dark web* yang melalui internet normal situs ini tidak dapat diakses, dalam mengakses situ ini diperlukan jaringan khusus seperti TOR *(The Onion Router)*. Didalam situs ini terdapat banyak kejahatan seperti *bounty hunter, drugs, human trafficking, hacker exploits, black market*, dan masik banyak kejahatan laiinya.

2.3 Mengenal *TOR (The Onion Router)*

Tor (The Onion Router) adalah jaringan *anonim* layaknya seperti bawang yang dirancang oleh karyawan di *US Naval Researce Laboratory (NRL)*. Hal ini dimplementasikan dengan menggabungkan teknologi peer-to-peer (P2P), dimana klien berkomunikasi dalam one-to-one, dengan teknologi *Sock* dalam menyampailkan TCP/IP dalam berkomunikasi. *Nod relay Tor* tersebar diseluruh dunia dan jaringan saat ini lebih dari 6000 *server*[10]. *Tor browser* menjadi salah satu *Software browser* yang *open source* digunakan untuk berselancar di internet khususnya *Deep web*. *Tor browser* dibangun melalui modifikasi *mozilla* dan memiliki pengaturan privasi dan keamanan tersendiri dengan konsep layaknya seuah bawang merah dan dapat mengakses situs .onion yang tidak dapat diakses oleh *browser* standar dan mesin pencari. *Tor* popular untuk kecepatan dan keamannya. *Tor* singkatan dari *The Onion Router* yang mengacu pada bawang dalam istilah teknis.

Tor merupakan *software open source* yang mudah untuk diunduh, dipasang, dan disetel. *Software Tor* dapat dipasang di *OS Windows*, *Mac OS* atau *Linux* dan bekerja pada semua jenis protokol internet seperti, HTTP, FTP, gopher dan lain-lain. Tor menyediakan kemampuan penelusuran canggih yang disebut *"hidden service"* untuk mendukung penelusuran anonim

2.4 Mengenal *dot Onion (.onion)*

Dot onion (.onion) merupan domain dari *Dark Web .onion* memperoleh nama sebagia data yang dikirim melewati berbagia lapisan enkripsi dan dekripsi layaknya lapisan bawang ketika dialihkan dari sumber ke tujuan. Tujuan dari penggunaan sistem ini adalah untuk membuat penyedia informasi dan orang yang mengakses informasi lebih sulit terdeteksi atau terlacak, oleh host jaringan menengah, atau oleh orang luar. Akan tetapi browser web seperti Tor dapat mengakses situs *dot onion (.onion)* dengan mengirim permintaan melalui jaringan server Tor dengan pemasangan perangkat lunak *proxy* yang sesuai. Mesin pencari *Deep Web* terhubung ke layanan lapisan *onion* melalui *Tor* dan *relay* dan kemudian memberikan hasil pencarian akhir ke *browser* di *Surface Web*[7].

2.5 *Text Preprocessing*

Tahapan seleksi pada sebuah data yang akan diseleksi pada sebuah dokumen, dalam memudahkan mengelola sebuah data yang belum terstruktur menjadi data yang terstruktur sesuan dengan

kebutuhan. proses *text preprocessing* terdiri dari beberapa tahap sebagai berikut :

1. ***Pertama***, *Case Folding*, merupakan proses pengubahan huruf pada sebuah dokumen menjadi satu bentuk, misalnya merubah huruf kapital dijadikan huruf kecil dan begitupun sebaliknya
2. ***Kedua,****Tokeninzing*, proses pemisahan teks menjadi potongan kalimat dan kata yang disebut *token*.
3. ***Ketiga,*** *Filtering*, proses dimana membuang kata dan tanda baca yang kurang bermakna secara signifikan, seperti penghilangan tanda *hashtag* (#), *url* dan tanda baca laiinya.

3. METODE PENELITIAN

Penelitian ini dilakukan dengan men-*capture* halaman-halaman *Dark Web*, dimana hasil *capture* halaman-halaman *Dark Web* kemudian akan analisis menggunakan *preprocesing text* dan menganalisis *vendor* yang berkaitan dengan frekuensi kata tertinggi. Untuk mendapatkan data dalam penelitian ini menggunakan salah satu aplikasi yaitu *Hunchly*. Adapun tahapan yang dilakukan pada penelitian ini melalui beberapa tahapan sebagia berikut :

1. Studi Pustaka

Studi pustaka dilakukan pada langkah awal untuk menghimpun informasi yang relevan dengan topik atau masalah yang akan diteliti. Sumber-sumber informasi pada studi pustaka dapat diperoleh melalui bukti fisik bukti fisik yang memiliki keterkaitan dengan masalah yang akan diteliti, jurnal ilmiah serta sumber-sumber informasi lainnya yang dapat diperoleh melalui internet.

2. Analisa Kebutuhan *Tools*

Tahapan ini dilakukan untuk menganalisis kebutuhan *tools* yang akan digunakan dalam penelitian meliputi proses-proses apa saja yang nantinya dapat dilakukan oleh *tools* yang dibutuhkan dalam analisis halaman-halaman *Dark web*, dalam hal ini penelitian menggunakan aplikasi *Hunchly* dan *Orange* dalam menganalisis untuk mendukung investigasi kejahatan, disamping itu dbutuhkan jaringan khusus dalam mengakses Dark web yaitu menggunakna jaringan *TOR (The Onion Router)* dan plugin *Hunchly* yang terinstall pada *browser Chrome*.

3. *Installasi* dan Konfigirasi

Tahapan ini dilakukan untuk menganalisis kebutuhan *tools* yang akan digunakan dalam penelitian meliputi proses-proses apa saja yg nantinya dapat dilakukan oleh *tools* yang dibutuhkan dalam menganalisis halaman-halaman *Dark Web* dalam mendukung investigasi Kejahatan, dalam hal ini penelitian menggunakan aplikasi *Hunchly* dalam men-*capture* halaman-halaman *Dark Web*, disamping itu configurasi jaringan menggunakan jaringan *TOR (The Onion Router)* agar dapat mengakses halaman-halaman *Dark Web*.

4. Pengumpulan Data

Tahapan selanjutnya adalah mendapatkan data halaman *Dark Web* dengan men-*capture* halaman-halaman *Dark Web* menggunakan aplikasi Hunchly. Proses mengumpulkan informasi dan data sebagai pendukung penelitian ini perlu ditetapkan tujuan yang melatarbelakanginya. Dengan menginputkan *selector* pada aplikasi *Hunchly* diharapkan dapat mengumpulkan data yang relevan.

5. Analisa Data

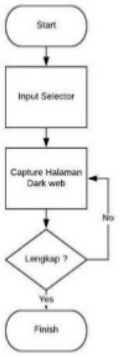
Dalam prose pengolahan datanya, hasil *capturing* halaman *Dark Web* berupa data halaman dan data jumlah *capture* berdasarkan *selector* yang ditampilkan pada *Desktop Hunchly*, data halaman hasil *capture* brupa file ".mhtml" yang kemudian dirubah menjadi .html dan di *convet* menjadi ".txt" dalam memudahkan Analisa data. Selanjutnya hasil *convet* data berupa ".txt" dilakukan analisa data menggunkan *preprocessing text* untuk mengetahui jumlah kata dari halaman yang berhasil di*capture* menggunakan aplikasi *orange* dimana data tersebut dilakukan *Case Foledering* yaitu proses pengubahan huruf dalam dokumen menjadi satu bentuk, misalnya huruf kapital dijadikan huruf kecil dan sebaliknya, selanjutnya dilakuakan *tokenizing* proses pemisahan teks menjadi potongan kalimat dan kata yang disebut *token*, dan selanjutnya *filtering* yaitu proses dimana membuang kata dan tanda baca yang kurang bermakna secara signifikan, seperti penghilangan tanda *hashtag* (#), *url* dan tanda baca lainnya tujuan dari proses ini memperoleh data yang lebih terstruktur.

6. Kesimpulan dan Saran

Tahapan ini merupakan tahapan akhir untuk menyampaikan kesimpulan dari temuan-temuan yang diperoleh selama penelitian. Laporan yang disusun diharapkan dapat memberikan gambaran dan informasi secara menyeluruh mengenai topik penelitian ini serta dapat memberikan rekomendasi yang bermanfaat untuk penelitian selanjutnya.

4. HASIL DAN PEMBAHASAN

Proses ini pengumpulan data halamana-halaman *Dark Web* yaitu dengan men-*capture* halaman-halaman *Dark Web* menggunkan aplikasi *Hunchly* dimana pada aplikasi *Hunchly* telah terinput *selector* halaman-halaman *Dark Web* yang telah dikunjungi dan kemudian *selector* akan menghitung halaman bedasarkan kata yang telah diinputkan pada *selector Hunchly*. Dalam hal ini peneliti menggolongkan *selector* berdasarkan case yang bebeda. Pada *case DarkMarket* 70 *selector*, *case CyperMarket* 42 *selector dan Case ApollonMarket* 58 *selector* kata yang dicari pada aplikasi *Hunchly* dengan tujuan memilah halaman yang relevan untuk dianalisis.



Gambar 1. Proses Pengumpulan Data

Contoh hasil *capture* halaman *Dark web* pada Gambar 1.

Gambar 2. Contoh *capture* halman dark web

Setelah data halaman-halaman *Dark Web* berhasil di *capture* dilanjutkan dengan menganalisa hasil *capture* halaman-halaman *Dark Web*, data yang diperoleh dari hasil *capture* disajikan pada Tabel 1

Tabel 1 Hasil *capture* halaman Dark Web

No	Halaman	Selector	Periode *Capturing*
1	5413 pages	162	15 April 2020 – 06 Mei 2020

Pada penelitian ini data yang diperoleh pada Tabel 1 kemudian dilakukan *preprocessing text* menggunakan aplikasi *orange* dengan tujuan menseleksi data agar data yang dipeloleh menjadi lebih terstruktur co22n hasil *preprocessing text* dari hasil ekstraksi data yang disajikan pada Gambar 2.

	Word	Word Count
1	)	2.32069e+06
2	(	2.31656e+06
3	=	1.95867e+06
4	;	757889
5	>	672172
6	3d	655967
7	/	522834
8	09	294144
9	.	254471
10	,	235440

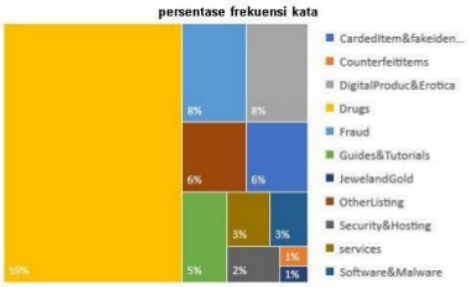
	Word	Word Count
1	drugs	69162
2	hashish	63804
3	cannabis	63254
4	stimulants	42732
5	security	41656
6	psychedelic	36606
7	goods	35616
8	c3	31779
9	opiates	31131
10	ecstasy	30857

Gambar 2. Hasil ekstraksi data halaman-halman Dark Web

Dari Gambar 4 dapat dilihat kata *"drugs"* memiliki frekuensi tertinggi dengan 69162 kata dari hasil ekstraksi halaman *Dark Web* yang berhasil ter-*capture*.

Gambar 3. Visualisasi berdasarkan banyaknya kata hasil *capture* halaman-halaman *Dark Web*

Berdasarkan hasil yang diperoleh seperti pada Gambar 3 hasil *preprocessing text* kemudian di klasifikasikan berdasarkan kategori dan divisulkan untuk melihat persentase dari masing-masing kategori.



Gambar 4. Persentase frekuensi kata

Berdasarkan hasil yang diperoleh pada perhitungan *preprocessing text* menggunakan aplikasi *orange* kata *"drugs"* memiliki persentase 59%, oleh sebab itu analisis terhadap *vendor* yang berkaitan dengan kata *"drugs"* menjadi prioraitas yang menjadi frekuensi kata paling besar. Selanjutnya dilakukan analaisis pada *vendor*, tahapan pertama yang dilakukan adalah dengan menganalisa pada *vendor* yang berhubungan dan menjual produk terkait dengan *"drugs"* Berikuat salah satu contoh gambar profil *vendor* yang menjual "drugs" seperti yang terdapat pada Gambar 5

Gambar 7. *Vendor*, *Seller level* dan *Trust level*

Tahapan berikutnya adalah melakukan analisa lebih mendalam terkait profil dari *vendor* tersebut seperti *TrusLevel* dan *SellerLevel*, Pada Gambar 7 dapat dilihat berupa data dari salah satu profil *vendor* pada halaman *Dark Web* yang berhasil ter-*capture*, pada tahapan proses selanjutnya dilakukan Analisa informasi data terkait *email* dan informasi-informasi lainnya yang dapat mendukung investigasi kejahatan, dalam hal ini aplikasi *Hunchy* mampu mengkategorikan data yang didapat dari hasil *capturing* halaman-halaman *Dark Web* berupa *email* dan url *Dark Web* yang terdapat pada halaman tersebut, contoh data yang diperoleh dari hasil *capturing* halaman *Dark Web* pada Gambar 8.

Gambar 8. Data Hasil *Capturing Hunchly*

Data yang dipeorleh dari hasil analisis empat *vendor* yang terkait dengan *"drugs"*, berikut daftar empat *vendor* dan data hasil analisis halaman *Dark Web* menggunkan *Hunchly* disajikan pada Tabel 2.

Tabel 2 Daftar *vendor* dan data *Dark Web*

Vendor	Data
SteroidWarehouse	• swgoodies@jabber.calyxinstitute.org • swgoodies@protonmail.com • www.swgoodies.com • Steroidwa7pp4iqw.onion
luck0923	• luck0923@protonmail.com
ConnectPL	• Connectpl_prv@protonmail.com • Pan.kowalski@gmail.com • _prv@protonmail.com
VanillaSurf	• vanillasurf@protonmail.com

Contoh detail hasil analisis *vendor* dari hasil analisis halaman *Dark Web* dalam mendukung investigasi kejahatan seperti yang terdapat pada Gambar 9 dan Gambar 10

Account, accountActivity,vendorLevel, trustLevel, memberSince, jabber, email, Website, PGP, Data

Gambar 9. Struktur data *vendor*

SteroidWarehouse, 06 May 2020, 2, 4, Jul 31 2019, swgoodies@jabber.calyxinstitute.org,swgoodies@protonmail.com, No Information, http://swgoodies.com & http://steroidwa7pp4iqw.onion, {$KEY}, {$DATA}

{$KEY}

-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBFSaiUUBEADLU7Uy9JgfYCrFO3RhmetOCDdsfXMKO+zv1N5/htELvTE8gqs1
GwV5Lz+CJ4SGZzhSCJBIXXiA74JJMLyUuew3vEcM9hK4Ah5u+CRL8hlob0mHPAzN
SDd8YhkYS7oaR3QNxmP0c43YzRRTwXc4kahP3ONj4gEtdvbN1RB3YrUGrvau9KOR
4w/J51aOAIJu7T4PTxeTg/isCSzhWsNAgdZDwWMaucemQe6GmO4k9LI6WgKQ1YwV
MyDMQOVSYdmGtLPvkFYp3m4mVNVgec5A4UcMILBh974BMtvZRP8S3nWIJ91R6kYy
PWIADqBscUQtzzbT7jZDfhftEg3SO+cd5CWRTN9kqueaqhdJQxoQrCi75avJ9Scw
9vv1/0odnxieOeA9v9HHPtDt6ujNAgRcViSgktysB6peSB/62qeFzWajkBx57KG/
uRrhChu4fGlSdS9Fae5GsoGjj51+hrZHk83Ki/7BgfpSeNCuheg/v2PfaQXF0DeA
n+/xTSB8UG0qLweMJpECll1jAjIKhIXEU1xaovG3sx3mojfhrrJvzV23u7zlxAnn
aJgc15HQbryvZuCQAz6sp+rCTjP8LPgxA5Z+rNjuZ78znGVfgVPlBcOCAfkcLt2h
h1YooCLxZC341le0CY6egUwZsp+BMPvGUWlSlnZm5/uYrdzH3BycIf//cQARAQAB
tBBTdGVyb2lkV2FyZWhvdXNlIiQ13BBMBCgAhBQJUmolFAhsDBQsJCAcDBRUKCQgL
BRYCAwEAAh4BAheAAAoJENFWXRUIidrUn5AQA1yBcu2/sx/GijKTpXb+fF+tH143
4CWjFpXGeEgGUhAyHQ/7kTXlLhbooEDIYconnxCOPhX8787PzAG7CXEtQFLrRx4/
s6KJK+29s1vJpBGwXEN6W58s9k3VyT+jF6Ot4Hxd2i6Tklk2MHrn+9qm6e0LyFpQ
50SyXP+Dg9ECHe0Me/UeQE7DsG8YBBO96qfg0pbNuaadN90mjS3Zvpt0UOHDK9HD
hDk+FX/UHQgqw66d5W4T8Z1kGsdKRXYeSGcejFTkrl7FNo8aUTydeJukmFX4OxrA
9SLcFJjvmkJPs8LIio9way91JB7wisgzMb1gqevU84JZeq0NAoboUSOdV/S6QZ6v
AjL7Ne8dGv/c7iU6j4gN3GX4LF70d3pmhLqvEcYyIvxzoQBg6KXHZQMxDAsnrhl+
Ov5nmChwXVV+G8meuBYenQbGNUSG90nmj3APInSC86lrtXrpym83494qH0tT65lq
f6Y7m5DAjMt+y6OT6C8S82R7hAsiq+SNYANwomhwB9k+cYHXR1lrLq06ZX+qwvL+
TosjaoOq59h3T3OVD/ia6YEqshUboFg8rxS83uee106GTwZEyexOJNwDTQhm6015
3ZPcmow6uQeIEcWdY8a2hwzhTjOyCdW8Y53yvQJ87wzPGE2WapBVcheyWtoAC2k7
eD3yzhdYdfhFW98puQINBFSaiUUBEAColB/bfAglAkhFNyBZ2Gq7YkSnYgaGR7CX
DqMZlIBnFXmjHCSXl47vVn4ZdDDDt8TGEzMUtLXZHRKnwAaG17rZxknLY6sY2Ze0
wG857zhFo+8j4+QhmViAIYBvLAXMEgjYQ63QimSXtv/yGNEfYkS0a7sXzrH25PRW
0L/r/oUSFaga5/IHezrHl1QvIBgAy6sebA7dS2VITaTSo1T2ms15aRj+xO9lMWq2
rZIVOYXSKX5gncSgvv67N6nK5fQfUTixGavKI+xW1b6y6+p1q/E4am0c1v8VFlZL
y3ie2K/PnjKMawNwSJ2PBRp4KtMDR6ienPVs3BOFzo6me/NLt4gvEGadRx9DTnAZ
dW1a1g6lc6kRCJVBWLqdtu2/Tb13pDsoWQjfD2+J9UYj43p7cUN6P1xbgcWgSnX5
nFuSP5VF/E7QbrKlSSeBopi/u70seXGsKiBJ1JQbkGmHUV2b6iw5KAAdrA6IjsGR
7eFmlwJ1XZ2bjNkbI9E5q5oHEvZn8ePo1BOB5Y2cg7nAFwKs3AXJu1QjRE629pL/
MLzOr2ygLu/WthDmQRdTVGs+p5fT6M1Qu5LkX5fUtyPfa/A/5Oxq2hHGdRBxiZ3/
ss7Vk21C/+gOEV4cPEVwA8Oqx65ELRej23hz67/YQAMifAQVDyr859OC3TVaUpPQ
RLhadueTOwARAQABiQIfBBgBCgAJBQJUmolFAhsMAAoJENFWXRUIidrUS9IQAJsK
shXxc3roEu5UaSdbYmo+gsBxR14q/906pV/7FyGUzUSYu1aMvG1nYuH0Lj9wx0JE
BLJxQsON+xxTadLY2woEs6ewvQY8uSR9/CykOTA/M7rxfpdHaPcE6w3AMJ3yX1a4
LXPcv9vxMIz+VEtbJo4v//c+4K9zyDTGHApYvWdKEHMcq2CS9K1Hdvjdh+TTx0ze
NdNRtxyfskrjlE2Cx1+Hl+aazQMFiE1z7xE6Tshwaf4h3bVOq/PnbKsSpdCnnqOy
91jJL6j+BRQF2qcu1o3ObOuokIKqh0BUb9DF8+GB3dCRKqzc0IUALDL+nxOZ5uod
7+mrKRAyy1xxK0w2m7KIPSCPRUtiL9ahmP0+K35M2OK4+xFSL+RDpwgL9TV7Q1BV
jvtX65TSGmNa109MHOUBRQ1lh90oXwF2x5bLcxqe3NuGTg51MmmhSWF9BAh+j0e6
e3RohszMTRe/BsUoQL4HYPzdfT1gQzYgrZFFT9Jr6P+HvRg41Hb1SA4Qz4yVCpHo
3RZuoTLxqNq7BtGkP+c22NzfofR1vMBs1QvPLzwYRLeA0mZBG2eavnU1+4pmka2i
xqlYdrMc1PMa0Q7VrNxw6VNS1MVTt8eEdvP+nvSIp6ECz28BXQmSxeQuNJKG1K5F
czpE19MpurFvGUEK2ikTdqd3TmVCJoWc00S05UIE
=8517
-----END PGP PUBLIC KEY BLOCK-----

{$Data}

##

CONTACT ME:

Jabber: swgoodies@jabber.calyxinstitute.org

E-Mail: swgoodies@protonmail.com

***Contact details:

Email: swgoodies@protonmail.com

Clearnet: www.swgoodies.com

Darknet: steroidwa7pp4iqw.onion

##

Gambar 10. Contoh hasil analisis data *vendor*

Berdasarkan analisis yang dilakukan menggunkan *preprocessing text* pada hasil *capture* halaman-halaman *Dark Web* dapat mengetahui prekuensi kata yang paling sering digunakan sehingga dapat menjadi dasar sekala prioritas peneliti terkait *vendor* yang akan dilakukan analisis halaman *Dark Web* dalam mendukung investigasi kejahatan.

Pada penelitian ini, sifat *Dark Web* yang terenkripsi berlapis dan anonim [11] menjadikan *Dark Web* tidak terindeks dimesin pencarian pada umumnya seperti *google, bing, dan yahoo* memerlukan analisis langsung pada halaman-halaman *Dark Web*, dengan menganlisis halaman *Dark Web* secara langsung dapat membantu dalam melakukan analisis halaman *Dark Web* dalam mendukung investigasi kejahatan. Dengan menggunakan aplikasi *Hunchly* maka mendapatkan informasi pada halaman *Dark Web* menjadi lebih

efisien. *Selector* yang terinput pada aplikasi *Hunchly* memudahkan dalam memperoleh data, memilah dan menganalisis halama-halaman *Dark Web*.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian yang telah dilakukan, untuk mejawab pertanyaan peneliti yang telah dikemukakan diawal, maka dapat diambil kesimpulan bahwa menganalisis halaman-halaman *Dark Web* menggunakan *Hunchly* dapat digunakan untuk melakukan analisa investigasi pada halaman *Dark Web*, dimana dari analisa halaman *Dark Web* ditemukan salah satu produk yang paling sering dijual yaitu *"drugs"* serta profil *vendor*.

Data *selector* yang terinput pada aplikasi *Hunchly,* dapat dijadikan sebagai dasar untuk mendapatkan informasi dari halaman *Dark Web*. Yang selanjutnya dilakukan analisa untuk mendapatkan informasi lebih mendalamdari tiap-tiap halaman *Dark Web*.

Berdasarkan hasil pada penelitian ini, didapatkan informasi yang penting untuk melakukan investigasi pada halaman *Dark Web,* seperti informasi tentang *profil pegguna, vendor level, trust level, membersince, jabber, email, website, PGP* yang semuanya dapat memberikan informasi terkait data yang dapat dijadikan sebagian salahsatu barang bukti dalam mendukung investigasi kejahatan.

Dari hasil penelitian, ditemukannya *email* vendor pada akun terkait sehingga perlu dilakukan investigasi yang kebih jauh terhadap akun untuk mendaatkan informasi yang relevan.

Saran untuk penelitian selanjutnya mengenai analisis halaman-halaman *Dark Web* menggunakn *Hunchly* mengunakan lebih banyak informasi dari forum-forum terkait yang terdapat dalam *Dark Web* untuk mendapatkan informasi yang lebih detail. Dalam penelitian selanjutnya dapat dilakukan dengan menggunakan *tools* lainnya untuk analisis halaman-halaman *Dark Web* dalam mendukung investiagsi kejahatan.

REFERENSI

[1] G. Hurlburt, "Shining light on the dark side of the Dark web," *IEEE Comput. Soc.*, vol. 1, 29 1, 2017.

[2] P. Shakarian, "Dark-web cyber threat intelligence: From data to intelligence to prediction," *Inf.*, vol. 9, no. 12, pp. 9–10, 16 2018.

[3] European Monitoring Centre for Drugs and Drug Addiction, *Drugs and the darknet*. 2017.

[4] K. Finklea, "Dark Web Kristin Finklea Specialist in Domestic Security," *Dark Web*, 2017.

[5] K. Kautsarina, "Perkembangan Riset Etnografi Di Era Siber : Tinjauan Metode Etnografi Pada Dark Web," *Masy. Telemat. Dan Inf. J. Penelit. Teknol. Inf. dan Komun.*, vol. 8, no. 2, p. 145, 2019.

[6] L. D. Larry Daniel, *Digital Forensic For 27 al Profesionals*. 2012.

[7] B. A. Abduljalil, "Critical Analysis of the Emerging Dark Web," no. April, 2017.

[8] S. Suneetha, "UNVEILING DEEP WEB , A HIGH-QUALITY , QUANTITATIVE INFORMATION RESOURCE," no. 2, pp. 167–174.

[9] D. Rathod, "Darknet Forensics," *Int. J. Emerg. Trends Technol. Comput. Sci.*, vol. 6 no. 4, pp. 77–79, 2017.

[10] M. Ganesan and P. Mayilvahanan, "Cyber Crime Analysis in Social Media Using Data Mining Technique," *Int. J. Pure Appl. Math.*, vol. 116, no. 22, pp. 413–4 15 2017.

[11] J. R. Harrison, D. L. Roberts, and J. Hernandez-Castro, "Assessing the extent and nature of wildlife trade on the dark web," *Conserv. Biol.*, vol. 30, no. 4, pp. 900–904, 2016.

1817-4874-1-SM

ORIGINALITY REPORT

17%	14%	2%	9%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	jurnal.fikom.umi.ac.id Internet Source	3%
2	www.analisis-data.com Internet Source	2%
3	islamindahdenganbelajar.blogspot.com Internet Source	2%
4	Submitted to Universitas Brawijaya Student Paper	1%
5	darknetlive.com Internet Source	1%
6	Anggit Ferdita Nugraha, Luthfia Rahman. "Meta-Algorithms for Improving Classification Performance in the Web-phishing Detection Process", 2019 4th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), 2019 Publication	1%
7	kamalrifasya.blogspot.com Internet Source	1%

8	eprints.ums.ac.id Internet Source	<1%
9	www.gammafisblog.com Internet Source	<1%
10	Submitted to Universitas Islam Indonesia Student Paper	<1%
11	Teresa Paulina Sihombing. "Tantangan Akuntan Di Era Revolusi Industri 4.0 Pada Masa Bonus Demografi Indonesia", Prosiding Seminar Nasional Riset Information Science (SENARIS), 2019 Publication	<1%
12	koreascience.or.kr Internet Source	<1%
13	hasanxch.blogspot.com Internet Source	<1%
14	amikhass.ac.id Internet Source	<1%
15	Submitted to Study Group Australia Student Paper	<1%
16	katalog.vse.cz Internet Source	<1%
17	eprints.umm.ac.id Internet Source	<1%

18	www.panamericanahoteles.cl Internet Source	<1%
19	www.ijrte.org Internet Source	<1%
20	jurnal.umk.ac.id Internet Source	<1%
21	tgskelompok10cybercrime.blogspot.com Internet Source	<1%
22	www.scribd.com Internet Source	<1%
23	abstrak.ta.uns.ac.id Internet Source	<1%
24	manualzz.com Internet Source	<1%
25	Submitted to iGroup Student Paper	<1%
26	Submitted to Liverpool John Moores University Student Paper	<1%
27	Submitted to University of Wales, Lampeter Student Paper	<1%
28	Submitted to UIN Sunan Ampel Surabaya Student Paper	<1%
29	Submitted to American Public University System Student Paper	

<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	Off		