

# ANALISIS SERANGAN BRUTE FORCE PADA IP ADDRESS CCTV (CLOSED CIRCUIT TELEVISION) MENGGUNAKAN METODE KOMPUTER FORENSIC

Segentar Alam<sup>1</sup>, Yesi Novaria Kunang<sup>2</sup>

Fakultas Ilmu Komputer Universitas Bina Darma

Email: segentaram06@gmail.com<sup>1</sup>, yesinovariakunang@binadarma.ac.id<sup>2</sup>

## ABSTRACT

*The science of computer network security related to investigations to determine the source of network attacks based on evidence log data, identification, analysis, and reconstruction of events is Network Forensics which is a branch of Digital Forensics. Brute Force Attacks are still one of the most popular password cracking techniques used to hack passwords. This attacks is done so that hackers have unauthorized access to get in to the system. In addition to Brute Force, password cracking can also be done with other techniques such as dictionary attacks, hybrids, and others. Although generally cracking passwords takes a long time, this attack has a fairly high success rate. One of the methods used to detect Brute Force Attacks is to use computer forensics methods. This method is used to identify and detect brute force attacks on CCTV (Closed Circuit Television) IP Address.*

**Keywords:** *Computer Forensic, Brute Force Attacks, CCTV, IP Address*

## ABSTRAK

Ilmu pengetahuan tentang keamanan jaringan komputer yang terkait dengan penyelidikan untuk menentukan sumber serangan jaringan berdasarkan data *log* bukti, identifikasi, analisis, dan rekonstruksi kejadian adalah Forensik Jaringan yang merupakan cabang dari Forensik Digital. *Brute force attack* masih menjadi salah satu teknik *cracking password* paling populer yang dilakukan untuk meretas kata sandi. Serangan ini dilakukan agar peretas memiliki akses tidak sah untuk bisa masuk ke dalam sistem. Selain *brute force*, *cracking password* juga dapat dilakukan dengan teknik lain seperti dengan *dictionary attack*, *hybrid*, dan lain-lain. Meskipun pada umumnya *cracking password* membutuhkan waktu yang cukup lama, namun serangan ini memiliki tingkat keberhasilan yang cukup tinggi. Salah satu metode yang digunakan untuk mengetahui serangan *brute force* yaitu menggunakan metode komputer forensic. Metode ini digunakan untuk mengetahui dan mendeteksi serangan brute force terhadap IP Address CCTV (*Closed Circuit Television*).

**Kata Kunci :** *Komputer Forensic , Brute Force Attack, Ip Address, CCT, IP Address*

## 1. PENDAHULUAN

Seiring perkembangan zaman, maka teknologi pun semakin maju. Di era ini kita mengenal teknologi komputer yang canggih, sehingga banyak dimanfaatkan di berbagai bidang kehidupan seperti contoh perkembangan teknologi perangkat *IoT*. *Internet of Things (IoT)* adalah suatu konsep dimana objek tertentu punya kemampuan untuk mentransfer data lewat jaringan tanpa memerlukan adanya interaksi dari manusia ke manusia ataupun dari manusia ke perangkat komputer [1]. *Internet of Things* lebih sering disebut dengan singkatannya yaitu *IoT*. *IoT* ini sudah berkembang pesat mulai dari konvergensi teknologi nirkabel, *micro-electromechanical systems (MEMS)*, dan juga Internet.



vital jaringan seperti server. Ketika *Tools* ini tidak ada pada jaringan maka forensik jaringan tidak dapat dilakukan.

2. **Detection**, pada tahapan ini alerts akan terjadi bila sistem mendeteksi suatu anomaly. Bila anomaly terjadi maka data anomaly tersebut akan dianalisa dengan berbagai ketentuan atau parameter. Setelah dianalisa maka akan ditentukan apakah anomaly tersebut serangan atau hanya trafik data normal. Apabila data trafik tersebut memang serangan maka proses forensik jaringan akan dilanjutkan namun apabila trafik data tersebut merupakan trafik normal yang artinya terjadi false alarm maka proses forensik jaringan dihentikan. *Tools* yang digunakan pada tahapan ini adalah *Wireshark, TCPDump, Snort, Bro, Pof, PADS, Ntop dan Sebek*.
3. **Incident response**, pada tahapan ini apabila terjadi serangan maka sistem akan merespon serangan tersebut. Respon sistem bergantung terhadap tipe serangan yang terjadi. Apabila serangan tersebut merupakan tipe serangan yang baru maka sistem akan mengumpulkan informasi tentang serangan tersebut untuk membuat suatu pertahanan apabila serangan tersebut menyerang kembali di masa yang akan datang. Pada tahapan ini akan ditentukan apakah proses forensik jaringan diteruskan atau dihentikan. Proses forensik jaringan dapat dihentikan ketika serangan yang menyerang merupakan serangan kecil dan bisa dilanjutkan apabila serangan tersebut mengakibatkan kerusakan sistem dan membutuhkan tindakan lebih lanjut untuk memperbaiki kerusakan tersebut.
4. **Collection**, pada tahapan ini data trafik akan dikumpulkan dari network security *Tools*. Tahapan ini sangat penting untuk mendapatkan jejak dari serangan yang terjadi karena data trafik akan berubah secara cepat dan jejak yang ditimbulkan oleh serangan tadi mungkin tidak akan terjadi lagi dilain waktu, sehingga pada tahap ini diperlukan hardware dan software yang cepat dan handal untuk mengumpulkan jejak serangan yang digunakan sebagai bukti. *Tools* yang bekerja pada tahap collection adalah *Wireshark, TCPDump, Snort, PADS, NfDump, Sebek, SiLK, TCPFlow dan Bro*.
5. **Preservation**, pada tahap ini data trafik hasil dari logs korban akan disimpan dalam sebuah perangkat backup. Data trafik ini akan disalin ke sebuah perangkat forensik jaringan untuk kemudian diuji coba melakukan serangan yang diduga apakah hasilnya akan sama atau tidak. Data trafik asli akan diawetkan sehingga tidak akan disentuh dan diuji coba, hal ini agar menjaga keaslian dari data trafik tersebut. *Tools* yang bekerja pada tahap ini ialah *Wireshark, TCPDump, Snort, PADS, NfDump, Sebek, SiLK, TCPFlow, dan Bro*.
6. **Examination**, pada tahap ini data trafik yang disalin tadi akan dilakukan analisis. Masalah yang sering terjadi pada tahap ini adalah informasi yang berlebihan dan waktu yang saling tindih dalam artian terjadi secara bersamaan sehingga memerlukan suatu perkiraan. Bukti yang terkumpul akan diekstrak untuk mendapatkan indikator yang spesifik dari serangan yang terjadi. *Tools* yang bekerja pada tahap ini ialah *Wireshark, TCPDump, TCPFlow, Flow-Tools, PADS, Argus, NfDump, Nessus, Sebek, Ntop, TCPTrace, NetFlow, Ngrep, SiLK, TCPStat, TCPDstat, TCPXtract, Pof, TCPReplay, Snort, Bro, dan Nmap*.
7. **Analysis**, pada tahap ini akan dilakukan analisa terhadap indikator yang didapatkan dari proses *examination*. Indikator-indikator ini akan dikumpulkan dan dicari hubungan antar indikator untuk menyimpulkan sebuah pengamatan dengan menggunakan pola serangan yang ada. Beberapa indikator penting akan berhubungan dengan pembentukan koneksi jaringan, *query DNS*, fragmentasi paket, protokol, dan sidik jari dari operasi sistem. Pola serangan akan disatukan, direkonstruksi dan dilakukan uji coba untuk mendapatkan informasi bagaimana serangan ini terjadi dan apa tujuan dari serangan. *Tools* yang bekerja pada tahap ini ialah *Wireshark, TCPDump, TCPFlow, Flow-Tools, PADS, Argus, NfDump, Nessus, Sebek, Ntop, TCPTrace, NetFlow, Ngrep, SiLK, TCPStat, TCPDstat, TCPXtract, Pof, TCPReplay, Snort, Bro, dan Nmap*.
8. **Investigation**, Pada tahap ini *network forensic investigator* akan menganalisa dan menentukan jalur yang dilalui oleh penyerang sampai ke jaringan korban. Data dari tahap analysis akan digunakan dan disatukan dengan data pada tahap ini untuk mendapatkan kesimpulan. Hasil

data trafik digunakan untuk mendapatkan atribut penyerangan dan menentukan identitas dari penyerang.

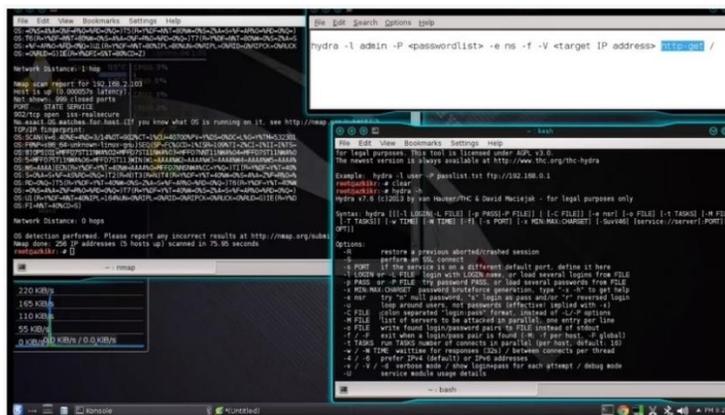
9. Presentation, tahap ini merupakan tahap akhir dari proses forensik jaringan. Pada tahap ini akan dipresentasikan hasil dari pengamatan terhadap data yang didapat. Bukti-bukti yang didapat akan dipresentasikan untuk mengadili pelaku penyerangan. Dan juga mempresentasikan bagaimana serangan tersebut terjadi dan bagaimana pola serangan tersebut sehingga dapat mencegah serang yang sama di masa yang akan datang.

### 3. HASIL DAN PEMBAHASAN

Pada hasil pengujian akan dilakukan *feature extraction* untuk melihat *attack pattern* serta melakukan validasi data hasil ekstraksi fitur dengan data hasil *capture* pada *wireshark*.

#### 3.1. Hasil Pengujian (Examination)

Hasil ini berdasarkan hasil uji coba *research* di laboratorium dengan menggunakan perangkat atau alat sesuai dengan kerangka berpikir di Bab III, dengan jarak 8 m dari CCTV target dan frekuensi sebesar 2,4 MHz dengan aliran *bandwith* sebesar 128 bps menggunakan aplikasi *route*, *Nmap*, *Hydra* dan *wireshark* yang menghasilkan parameter yang telah di uji (lihat Gambar 2).



Gambar 2. Tools yang digunakan untuk exploit CCTV

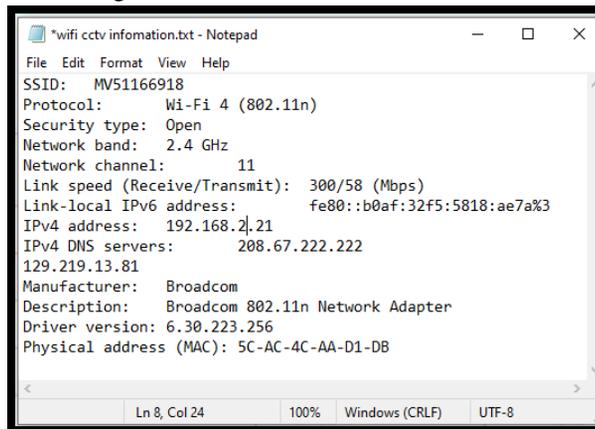
#### 3.2. Tools Route

Tools tersebut digunakan untuk menghasilkan alamat IP domain dengan mengetikkan *route -n* di terminal, sehingga nama domain tujuan untuk alamat IP. Hasil dari tersebut dapat dilihat pada gambar 3.



**Gambar 3.** Hasil Informasi Jalur Jaringan yang di gunakan CCTV

Adapun cara kedua untuk mendapatkan informasi alamat IP bisa langsung koneksi ke wifi CCTV yang aktif di jaringan di karena sering dikonfigurasi secara otomatis yang dihasilkan bentuk informasi pada gambar 4. sebagai berikut:



**Gambar 4.** Informasi Wifi CCTV

### 3.3. Tools Nmap

*Nmap* adalah sebuah aplikasi atau tool yang berfungsi untuk melakukan port scanning, antara lain mengumpulkan informasi setiap host atau CCTV yang hidup pada jaringan local; mengumpulkan informasi setiap ip address pada jaringan local; mengumpulkan informasi setiap sistem operasi pada host maupun seluruh host pada target jaringan menemukan setiap port yang terbuka dari host target; menemukan adanya infeksi dari virus maupun malware; mengumpulkan informasi mengenai layanan-layanan (service) pada host terget dan server pada jaringan target. Hasil dari semua informasi tersebut dapat dilihat pada gambar di bawah ini.

```
File Edit View Bookmarks Settings Help
192.168.178.0 0.0.0.0 255.255.255.0 U 0 0 0 vnet1
root@backlikr: # nmap -sS -O 192.168.2.1/24
Starting Nmap 6.40 (http://nmap.org) at 2014-09-14 21:18 SGT
Nmap scan report for R22.alfa.com [192.168.2.1]
Host is up (0.0000s latency)
Not shown: 996 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
5555/tcp  open  freeciv
MAC Address: 00:0C:CA:74:70:50 (ALFA)
Device type: general purpose
Running: Linux 2.6.x
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.17 -- 2.6.36
Network Distance: 1 hop

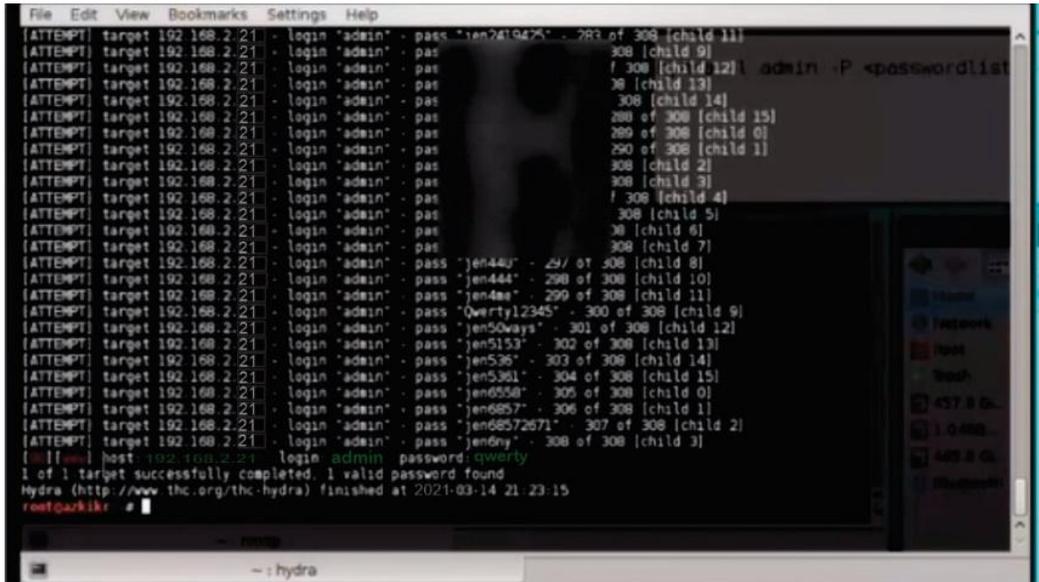
Nmap scan report for 192.168.2.21
Host is up (0.014s latency)
Not shown: 997 closed ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
7777/tcp  open  http
MAC Address: 28:10:70:14:BF:3C (D-Link International)
Device type: general purpose
Running: Linux 2.6.x
OS CPE: cpe:/o:linux:linux_kernel:2.6
-- : nmap
```

Gambar 5. Hasil Informasi Port yang di gunakan untuk celah kebocoran

Informasi yang di dapatkan di dalam jaringan dengan menggunakan tools Nmap di dapatkan IP target yang berada dalam satu jaringan dengan menggunakan alamat logic 192.168.2.21 dengan port 80 dan 443 melalui aplikasi layer dan mempunyai celah port 7777.

### 3.4. Tool Hydra

Hydra adalah satu tool security yang dipakai untuk melakukan cracking password secara remote. Hydra ini merupakan tool yang disediakan untuk menguji keamanan yang dapat dipakai untuk mencari password (menguji apakah password aman). Untuk melakukan penetration test menggunakan tool hydra yang dilakukan menetikkan satu perintah yaitu “**hydra -l admin -P <passwordlist> -e ns -f -V <target IP address> http-get /**”. Dimana **hydra -l admin -P <passwordlist>** adalah perintah untuk mengetahui list password, sedangkan list password merupakan nama file, dan **<target IP address>** adalah IP address dari target, serta http-get adalah service target CCTV. Yang di dapatkan nama user: admin dan passwordnya adalah qwerty. Dapat dilihat jelas pada gambar 6.

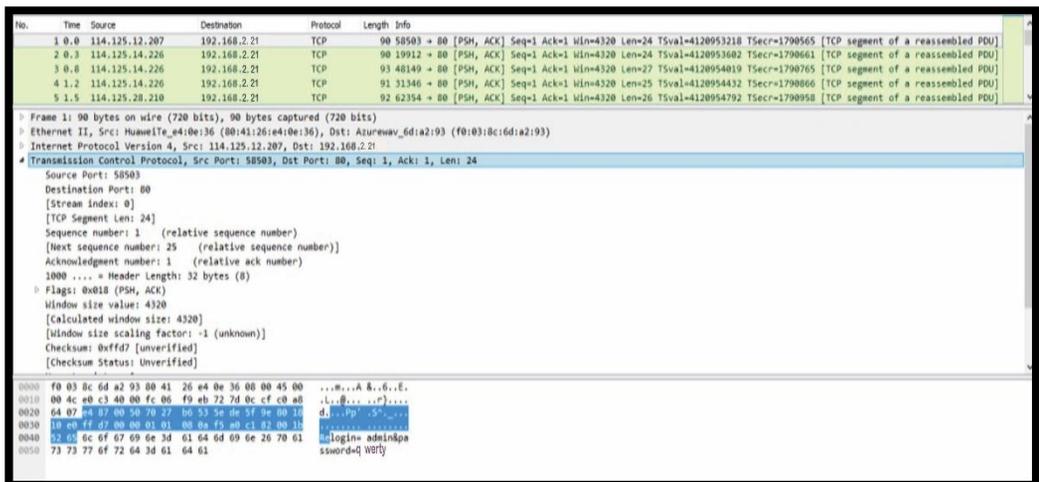


Gambar 6. Hasil Penetration Password CCTV target

Pada gambar 6. menjelaskan bahwa tools hydra yang di gunakan sebagai serangan bluforce melalui wordlist dapat mampu menembus semala 21 menit 23 detik lamanya.

### Wireshark

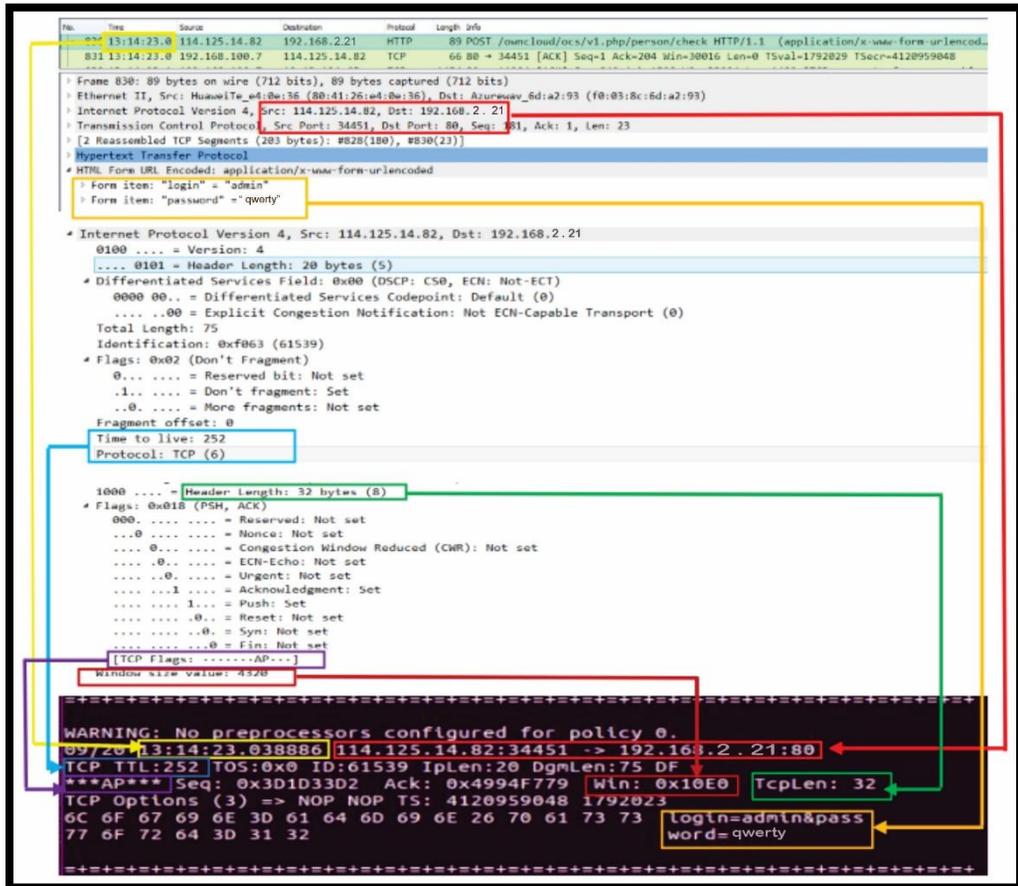
Wireshark yaitu *Network Protocol Analyzer*, termasuk juga kedalam satu diantara *network analysis tool* atau *packet sniffer*. Wireshark disini digunakan sebagai mengamati data dari jaringan yang tengah beroperasi (*capture traffic*) atau dari data yang ada di disk, dan segera melihat atau mensortir data yang tertangkap, mulai dari informasi singkat dan rincian untuk segala hal tentang paket termasuk full header dan jumlah data. Capture traffic yang dilakukan dalam jenis file packet capture (pcap), penelitian dilanjutkan dengan melakukan feature extraction berfungsi untuk membuat file *comma separated Value (CSV)* dari raw data hasil capture wireshark (pcap) yang bertujuan untuk mengenali pola serangan dari dataset yang telah dilakukan, dari hasil penyerangan dengan teknik brute force dari hasil analisis yang dilakukan wireshark dapat di tangkap. Yang dapat dilihat pada gambar di bawah ini:



Gambar 7. Hasil traffic jaringan

### 3.5 Analisa (Analysis)

Analisa ini yaitu mengambil pendekatan metode dalam menghasilkan kesimpulan yang berkualitas berdasarkan pada ketersediaan atau bahkan sebaliknya, dengan menyimpulkan bahwa tidak terdapat kesimpulan/hasil yang diperoleh dan hal tersebut mungkin saja akan terjadi Ketika menghadapi situasi real dilapangan. Data-data real dilapang yang dihasilkan dari monitoring atau capture traffic menggunakan wireshark Adapun parameter yang diambil yaitu no\_paket, time\_service, ip\_src, ip\_dst, port\_src, port\_dst, windows, flags, ttl, iplen, packetlen, protocol.



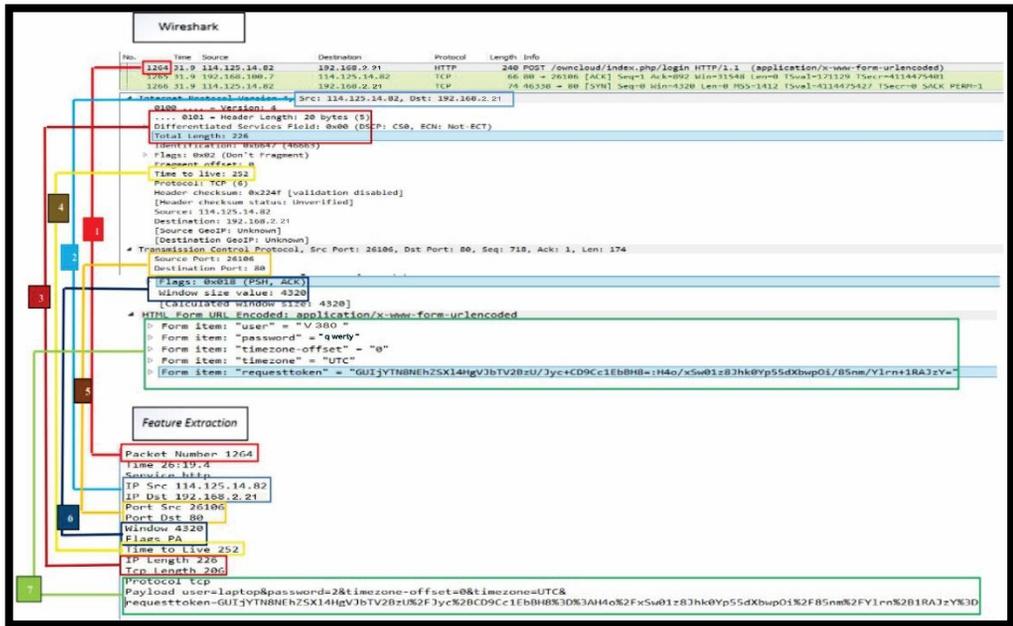
Gambar 8. Hasil Analisa Exploit CCTV Di Jaringan

### 3.6 Investigation

Terdapat 7 point persamaan data antara hasil future extraction dengan raw data (pcap) yang di hasilkan dari tool wireshark berikut penjelsanya mengenai tujuh point data yang sama pada hasil feature extraction dan raw data (pcap):

1. Nomor satu (1) berisikan nomor paket atau frame dari paket data. Pada gambar 4.8. nomor paket bernilai 1264
2. Nomor dua (2) berisikan ip address source dan destination dari paket data. Pada gambar 4.8. ip address source adalah 114.125.14.82 dan ip address destination 192.168.2.21
3. Nomor tiga berisikan ip length dan tcp length dari paket data. Nilai ip length adalah 226. Untuk mendapatkan nilai tcp length, nilai ip length dikurangi nilai header length dalam hal ini 20 sehingga nilai tcp leng 206.

4. Nomor empat (4) berisikan nilai *time to live* (ttl) dari paket data dengan nilai 252
5. Nomor (5) berisikan nilai *source port* dan *destination port* dari paket data. *Source port* bernilai 26106 dan *destination port* bernilai 80.
6. Nomor enam (6) berisikan nilai *flags* dan *window* dari paket data. nilai *flags* adalah PSH, ACK (PA) dan nilai *window* adalah 4320.
7. Nomor tujuh (7) berisikan *payload* dari paket data. *Payload* berisi *user* = laptop, *password* = 2, *timezone-offset* = 0, *timezone* = UTC, dan *requesttoken* = GUIjYTN8NEhZSX14HgVJbTV2BzU%2FJyc%2BCD9Cc1EbBH8%3D%3AH4o%2FxFsw01z8Jhk0Yp55dXbwpOi%2F85nm%2FYln%2B1RAJzY%3D.



Gambar 9. Hasil Investigasi pcap lalu Lalang jaringan terdeteksi wireshark

Pada hasil *feature extraction* terdapat 14 fitur yang diekstrak dari *raw data* (pcap) hasil skenario pengujian yang akan dianalisis untuk menentukan polaserangan dan pola akses normal. Fitur tersebut adalah; *packet number*, *timestamp*, *service*, *ip source*, *ip destination*, *port source*, *port destination*, *windows*, *flags*, *ttl*, *ip length*, *payload*, *tcp length*, dan *protocol*. Berikut adalah hasil *feature extraction* dari *raw data* (pcap) hasil pengujian berdasarkan scenario.

Tabel 1. Nilai Fitur Pada Skenario Pengujian

| Ip dst       | Port dst | flags | ttl | Protocol |
|--------------|----------|-------|-----|----------|
| 192.168.2.21 | 80       | PA    | 252 | TCP      |

Table 2. Nilai Fitur IP Length dan TCP Length

| Window              | Ip Length      | Tcp Length              |
|---------------------|----------------|-------------------------|
| 4320, 11855, 27960, | 226, 218, 214, | 206, 198, 194,196, 922, |
| 35493, 43025, 50555 | 216, 942, 950, | 930,93, 748             |
|                     | 113, 768       |                         |

Pada tabel 1 dan 2 disimpulkan pola akses normal dari skenario pengujian memiliki pola nilai *ip address destination*, *port destination*, *flags*, *time to live*, *protocol* yang sama dan dengan rentang

nilai *ip length* 113 sampai 1023. Dari hasil *feature extraction raw data* (pcap) serangan *brute force* menggunakan kali linux terdapat fitur dengan nilai yang sama dan nilai yang berbeda.

### 3.7. Presentasi Dalam Bentuk Pembahasan

Presentasi adalah tahapan akhir dari proses forensic jaringan, dalam tahapan ini merepresentasikan informasi yang merupakan hasil dari proses Analisa. Proses reporting yang digunakan identifikasi actionable information yang di peroleh dari data-data terdahulu yang nantinya bisa sebagai informasi yang dapat digunakan untuk keperluan mendatang misalnya tujuan keamanan seperti backdoor yang mungkin bisa dieksploitasi, maka dibutuhkan penanganan segera mungkin seperti *policy shortcomings* atau *procedural errors formal review* dapat membantu dalam mengidentifikasi dan meningkatkan kualitas. Hasil dari pengujian yang dilakukan berhasil di tangkap wireshark dapat digunakan untuk membaca hasil *log* yang dihasilkan 136 *alert* paket data dari total jumlah paket 13.650 paket. *Worldlist* yang digunakan pada scenario pengujian ini memiliki 111 kata sehingga serangan brute force yang dilakukan sebanyak 111 kali.

## 4. KESIMPULAN

Adapun hasil dari analisis penelitian ditarik beberapa kesimpulan sebagai berikut :

1. Dari hasil serangan menggunakan *Brute Force* pada IP Address CCTV dengan type V380 menggunakan aplikasi hydra pada OS kali linux dapat berhasil dilakukan dengan mendapatkan IP Address CCTV 192.168.1.1 dengan *protocol tcp*, port 7777.
2. Pola serangan *Brute Force* pada IP CCTV memiliki beberapa nilai fitur yang sama yaitu: *protocol* "tcp", *flags*"PA", *window* "4320", *ttl*"252", *ip length* "113-1023".
3. IP Address CCTV tipe v380 ini aktif wirelessnya secara default yang dapat mudah diakses pengguna yang tidak sah yang memiliki masih memiliki celah walaupun sudah memiliki security LDAP didalamnya.

## DAFTAR PUSTAKA

- [1] Dewawebtim, "Internet of thing's," incdewaweb. Jakarta, 2021. [Online].
- [2] G. H. Cahyono, "INTERNET OF THINGS (SEJARAH, TEKNOLOGI DAN PENERAPANNYA)," *FORUM TEKNOLOGI*, vol. 6, no. 2, pp. 35-41, 2016.
- [3] J. Cieszynski, *Closed Circuit Television CCTV Installation, Maintenance and Operation*, Amsterdam: Elsevier Science, 2003.
- [4] I. Gunawan, "PENGUNAAN BRUTE FORCE ATTACK DALAM PENERAPANNYA PADA CRYPT8 DAN CSA-RAINBOW TOOL UNTUK MENCARI BISS," *InfoTekJar (Jurnal Nasional Informatika dan Teknologi Jaringan)*, vol. 1, no. 1, pp. 52-55, 2016.
- [5] Mustapha and dkk, "Brute Force Attack Detection and Prevention on a Network Using Wireshark Analysis," *Jurnal Engineering Sciences & Research Technology*, vol. 6, no. 6, pp. 26-37, 2017.
- [6] Deris and dkk, "Investigating Brute Force Attack Patterns in IoT Network," *ournal of Electrical and Computer Engineering*, pp. 1-13, 2019.
- [7] Feradhita, *Brute Force dan metode yang digunakan*, Jakarta: Komit, 2020.