BINA DARMA CONFERENCE ON Computer Science

Volume 3, Number 3, 2021


Diterbirkan Oleh:
Direktorat Riset dan
Pengabdian kepada Masyarakat
Universitas Bina Darma

Diselenggarankan Oleh:
Fakultas Ilmu Komputer Universitas Bina Darma

pISSN: 2685-2675 eISSN: 2685-2683

Bina Darma Conference on Computer Science
p-ISSN: 2685-2675
e-ISSN: 2685-2683




**Published:** 2021-11-03

## Articles

Download PDF

## KLASIFIKASI MALWARE DENGAN RECURRENT NEURAL NETWORK

Desi Efriyani, Febriyanti Panjaitan, Muhamad Akbar, Aan Restu Mukti

423-430

Download PDF

## IMPLEMENTASI ALGORITMA FISHER YATES SHUFFLE PADA APLIKASI BELAJAR HURUF HIJAIYAH

Irfan Kurniawan, Siti Sauda

431-440

Download PDF

## ANALISIS KEAMANAN JARINGAN PADA LAYANAN INTERNET PUBLIK MENGGUNAKAN METODE PENETRATION TESTING EXECUTION STANDARD (PTES) DPRD PROVINSI SUMATRA SELATAN

Angga Pratama, Dedy Syamsuar

441-446

Download PDF

## PENGEMBANGAN APLIKASI PENDUKUNG SISTEM INFORMASI ADMINISTRASI KEPENDUDUKAN REGISTER PENGGUNAAN PADA MESIN ANJUNGAN DUKCAPIL MANDIRI

Muzakir Muzakir, Nurul Adha Oktarini Saputri

447-453

Download PDF

## ANALISIS KUALITAS WEBSITE SMA NEGERI 4 PALEMBANG MENGGUNAKAN METODE WEBQUAL 4.0

Putri Mayang Sari, Nyimas Sopiah

454-459

Download PDF

## PERANCANGAN DATA MART KEPEGAWAIAN BINA DARMA

Derwanto Derwanto, Susan Dian Purnamasari

460-467

Download PDF

## SISTEM INFORMASI PENDATAAN DAN PEMANTAUAN TANAMAN PADA PT. KENDI ARINDO

## PERKEBUNAN BERBASIS ANDROID

Juanda Syaputra Nasution, Novri Hadinata

468 - 474

Download PDF

## Analisis Sistem Informasi Akademik (SIAKAD) STIE Serasan Terhadap Kepuasan Pengguna Dengan Menggunakan Metode End User Computing Satisfaction (EUCS)

Sekolah Tinggi Ilmu Ekonomi Serasan Muara Enim

Hartati Amaliah, Evi Yulianingsih

475-483

Download PDF

## IMPLEMENTASI E-LEARNING DALAM PEMANFAATAN MOODLE (STUDI KASUS : SMK PELAYARAN SINAR BAHARI PALEMBANG)

SMK PELAYARAN SINAR BAHARI PALEMBANG

Dian Istiningsih, Iin Seprina

484-490

Download PDF

## Penerapan metode customer satisfaction index dan service quality untuk mengukur kepuasan pembaca terhadap kualitas layanan website intens.news

Studi kasus pada media online intens.news

Sulistri ., Kurniati Kurniati

491-498

Download PDF

## Media Pembelajaran Interaktif Bahasa Korea Berbasis Multimedia

Andariga Martha, Deni Erlansyah

499 - 508

Download PDF

## WEBSITE INFORMASI SEKOLAH MENGGUNAKAN CONTENT MANAGEMENT SYSTEM PADA MA TIJAROTAL LANTABUR

Renta Saputra, Kurniawan Kurniawan

509-516

Download PDF

## Analisis Pemanfaatan E-learning Sebagai Media Pembelajaran Di SMK Negeri 1 Tanjung Lago Menggunakan Metode Technology Acceptance Model (TAM)

SMK Negeri 1 Tanjung Lago

Ica Arisa, Evi Yulianingsih

517-527

Download PDF

## VISUALISASI DATA LOKASI RAWAN BENCANA DI PROVINSI SUMATERA SELATAN MENGGUNAKAN TABLEAU

Studi kasus pada badan penanggulangan bencana daerah (BPBD)

Septy Angreini, Edi Supratman

528-534

Download PDF

## ANALISIS TINGKAT KEPUASAN PENGGUNA SISTEM LAYANAN KEPENDUDUKAN DAN PENCATATAN SIPIL OGAN ILIR PADA KECAMATAN PEMULUTAN MENGGUNAKAN METODE PIECES FRAMEWORK

Sri Mulyani, Fatoni Fatoni

535-543

Download PDF

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

Segentar Alam, Yesi Novaria Kunang

544-553

Download PDF

## PERANCANGAN APLIKASI MOBILE ANDROID BERBASIS UNTUK KASIR PADA KEDAI RASA KOPI PALEMBANG

Muhammad Azhari, Linda Atika

554-559

Download PDF

## USABILITY TESTING SISTEM INFORMASI AKADEMIK (SISFO) PADA MAHASISWA BINADARMA MENGGUNAKAN USE QUESTIONNAIRE (STUDI KASUS MAHASISWA PROGRAM SISTEM INFORMASI)

STUDI KASUS MAHASISWA PROGRAM SISTEM INFORMASI

Nugroho Wisnu Mukti
560-568

Download PDF

## PEMANFAATAN DATA MINING UNTUK MEMPREDIKSI KELULUSAN UJI KOMPETENSI SMK JURUSAN TEKNIK KOMPUTER JARINGAN DI SMK SETIA DARMA PALEMBANG DENGAN ALGORITMA C 4.5

Andre Andre, Edi Surya Negara
569-576

Download PDF

## THE SISTEM INFORMASI PENGADUAN SARAN DAN MASUKAN (SIAP SAMA) PADA BADAN PUSAT STATISTIK KABUPATEN MUSI BANYUASIN

BADAN PUSAT STATISTIK KABUPATEN MUSI BANYUASIN

EKO SUSANTO, Muhamad Ariandi
577-586

Download PDF

## THE SISTEM INFORMASI PENGAJUAN PELAYANAN DATA PADA BADAN PUSAT STATISTIK KABUPATEN MUSI BANYUASIN DENGAN METODE RATIONAL UNIFED PROCESS (RUP)

BADAN PUSAT STATISTIK KABUPATEN MUSI BANYUASIN

Imam Arifin, Muhamad Ariandi
587-594

Download PDF

## Sistem Informasi Presensi Online Mendukung Work From Home Berbasis Android Pada Bank BTN Syariah Palembang

Studi Kasus Pada Bank BTN Syariah Palembang

Muhammad Dicky Ramadhan, Kurniawan Kurniawan
595-604

Download PDF

## ANALISIS SYSTEM E-BILLING UNTUK PEMBAYARAN PAJAK UNTUK MENINGKATKAN KEPUASAN PENGGUNA PADA KANTOR PELAYANAN PAJAK PRATAMA PALEMBANG

Abdul Basir, Nia Oktaviani
605-613

Download PDF

## ANALISA PENERIMAAN WEB PROFIL SMA NEGERI 8 PALEMBANG DENGAN METODE TECHNOLOGY ACCEPTANCE MODEL (TAM)

Aswan Habibi, Linda Atika

614-619

Download PDF

## ANALISIS KUALITAS LAYANAN WEBSITE SEKOLAH TINGGI TEKNOLOGI PAGARALAM DENGAN MENGGUNAKAN METODE WEBQUAL 4.0

Doni Dahrul, Edi Yulianingsih

620-626

Download PDF

## ANALISIS SISTEM INFORMASI BADAN PENGELOLAAN KEUANGAN DAN ASET DAERAH SUMATERA SELATAN BERBASIS WEB MENGGUNAKAN METODE EUCS

Muhammad Febriyanto, Tri Oktarina

627-631

Download PDF

## Winda Laili Nur Khafifah, Fatoni ANALISIS DAN KEPUASAN PENGGUNA SIAKAD YAYASAN PERGURUAN SERASAN MUARA ENIM MENGGUNAKAN METODE WEBQUAL 4.0

Winda Laili Nur Khafifah, Fatoni Fatoni

632-641

Download PDF

## ANALISIS KEPUASAN PENGGUNA WEBSITE DINAS PENDIDIKAN BANYUASIN DENGAN MENGGUNAKAN METODE WEBQUAL 4.0

Khoiru Falupi, Nyimas Sopiah

642-647

Download PDF

**Seminar Daring BDCCS**

**Form Registrasi Seminar Daring**

**Template Artikel**


**Tutorial Submit Article**


**Tutorial Reviewer**


**Form Pilihan Publikasi**


**Biaya Pendaftaran**

Biaya Seminar BDCCS

**Rp. 275.000**

Biaya Yudisium

**Rp. 400.000**

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

**Segentar Alam[1], Yesi Novaria Kunang[2]**
Fakultas IlmuKomputer Universitas Bina Darma
Email: segentaralam06@gmail.com[1] ,yesinovariakunang@binadarma.ac.id[2]

***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

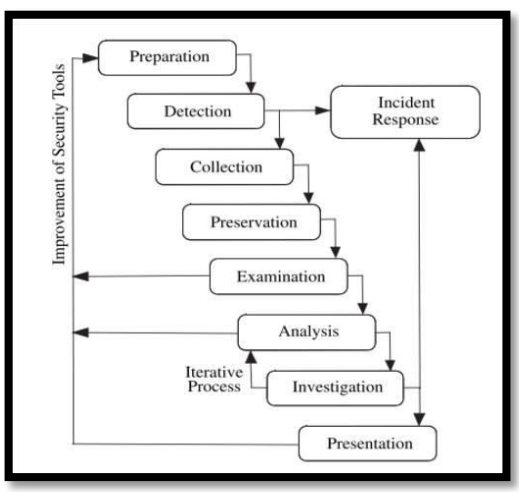
Seiring perkembangan zaman, maka teknologi pun semakin maju. Di era ini kita mengenal teknologi komputer yang canggih, sehingga banyak dimanfaatkan di berbagai bidang kehidupan seperti contoh perkembangan teknlogi perangkat *IoT*. *Internet of Things (IoT)*adalah suatu konsep dimana objek tertentu punya 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.

*IoT* ini juga kerap diidentifikasikan dengan RFID sebagai metode komunikasi [2]. Walaupun begitu, *IoT* juga bisa mencakup teknologi-teknologi sensor lainnya, semacam teknologi nirkabel maupun kode QR yang sering kita temukan di sekitar kita. Seperti contoh perangkat *IoT* yang sering digunakan untuk keamanan ruangan dan lalu lintas jalan raya yaitu *cctv*. *Closed Criuit Television* atau *cctv* memiliki arti yaitu menggunakan sinyal yang bersifat tertutup atau rahasia, tidak seperti televisi biasa pada umumnya yang merupakan *broadcast signal* [3]. *CCTV* memiliki fungsi sebagai umumnya digunakan untuk pelengkap.

Sistem keamanan dan juga banyak dipergunakan di berbagai lokasi seperti bandara, kemiliteran, kantor, pabrik, toko, dan laboraturium komputer. Namun, CCTV juga memeiliki Internet Protocol Address atau yang sering disingkat IP Address yang rentan dari serangan keamanan jaringan. Serangan terhadap IP Address *CCTV* yang paling sederhana yaitu *Brute Force Attack*. Serangan brute-force adalah sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin [4]. Berhasil atau tidaknya serangan bergantung pada kumpulan dari jumlah kemungkinan *password* yang telah ditetapkan. Jika jumlah kemungkinan *password* yang ditetapkan banyak maka serangan *brute force* mempunyai kemungkinan berhasil yang tinggi tetapi akan memakan lebih banyak waktu [5]. Jika dalam *word list* yang digunakan terdapat kata yang cocok dengan *password* maka serangan *brute force* berhasil dilakukan. Serangan orang dalam /internal lebih banyak berasal dari jaringan internal yang membahayakan seluruh sistem keamanan IoT [6]. Salah satu cara mendekteksi serangan *brute force* yaitu dengan melakukan komputer forensik.

## 2. METODOLOGI PENELITIAN

Dalam penelitian ini metode penelitian yang digunakan adalah metode forensik jaringan. Dalam melakukan forensik jaringan terdapat beberapa tahapan diantaranya yaitu: Persiapan (*Preparation*), deteksi (*Detection*), tanggapan insiden (*Incident response*), Pengumpulan data (*Collection*), kelestarian data (*Preservation*), Pengujian (*Examination*), Analisis (*Analysis*), Penyidikan (*investigation*), dan presentasi (*Presentation*) [7]. Seperti yang digambarkan dalam alur metodologi berikut ini:




**Gambar 1.** Tahapan Metodologi Forensik Jaringan

1. Preparation, forensik jaringan akan dapat bekerja ketika network security *Tools* seperti firewalls, packet analyzers, intrusion detection system dipasang dan disebar pada titik-titik

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

2. Detection, pada tahapan ini alerts akan terjadi bila sistem mendeteksi suatuanomaly. 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, P0f, PADS, Ntop dan Sebek*.
3. Incident response, pada tahapan ini apabila terjadi serangan maka system 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 networksecurity *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, P0f, 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 iniialah *Wireshark, TCPDump, TCPFlow, Flow-Tools, PADS, Argus, NfDump,Nessus, Sebek, Ntop, TCPTrace, NetFlow, Ngrep, SiLK, TCPStat, TCPDstat,TCPXtract,P0f, 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.

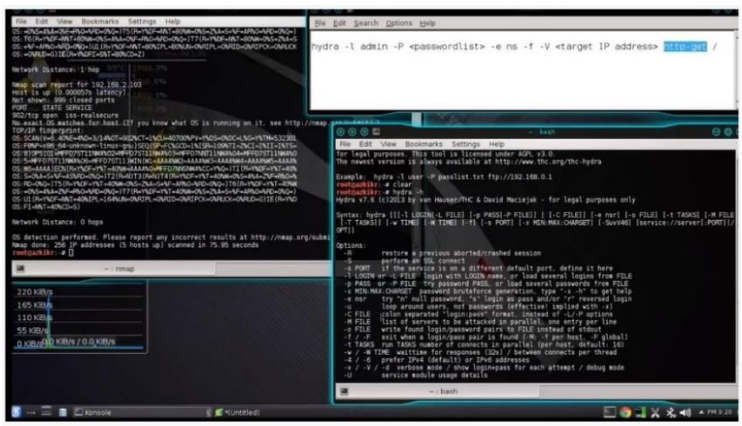
9. Presentation, tahap ini merupakan tahap akhir dari proses forensik jaringan. Pada tahap ini akan dipresentasikan hasil dari pengamatan terhadap data yang didapat. Bukti-bukti yang didapat akan dipresentasikan untuk mengadili pelaku penyerangan. Dan juga mempresentasikan bagaimana serangan tersebut terjadi dan bagaimana pola serangan tersebut sehingga dapat mencegah serangang 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 ektraksi fitur dengan data hasil *capture* pada *wireshark*.

### *3.1. Hasil Pengujian (Examination)*

Hasil ini berdasarkan hasil uji coba *reserch* 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).



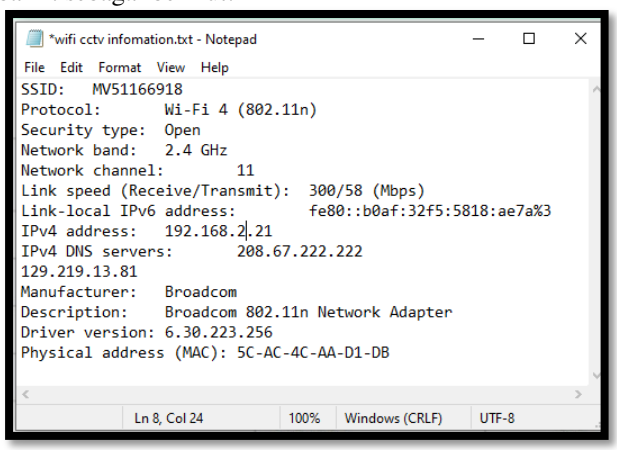
**Gambar 2.** Tools yang digunakan untuk *exploit CCTV*

### *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*

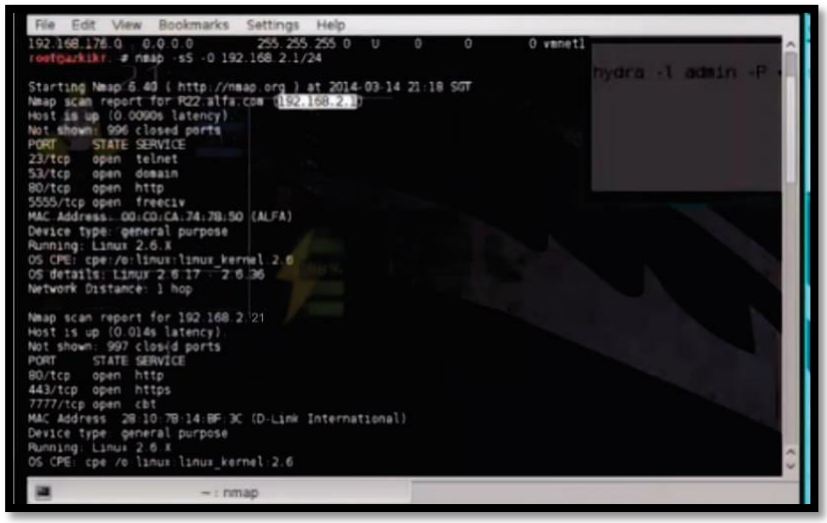
Adapun cara kedua untuk mendapatkan informasi alamat IP bisa langsung koneksi ke wifi CCTV yang aktif di jaringan di karena sering dikonfigurasi secara otomatis yang dihasilkan bentuk informasi pada gambar 4. sebagai berikut:




**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 setipa ip address pada jaringan local; mengumpulkan infromasi 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.

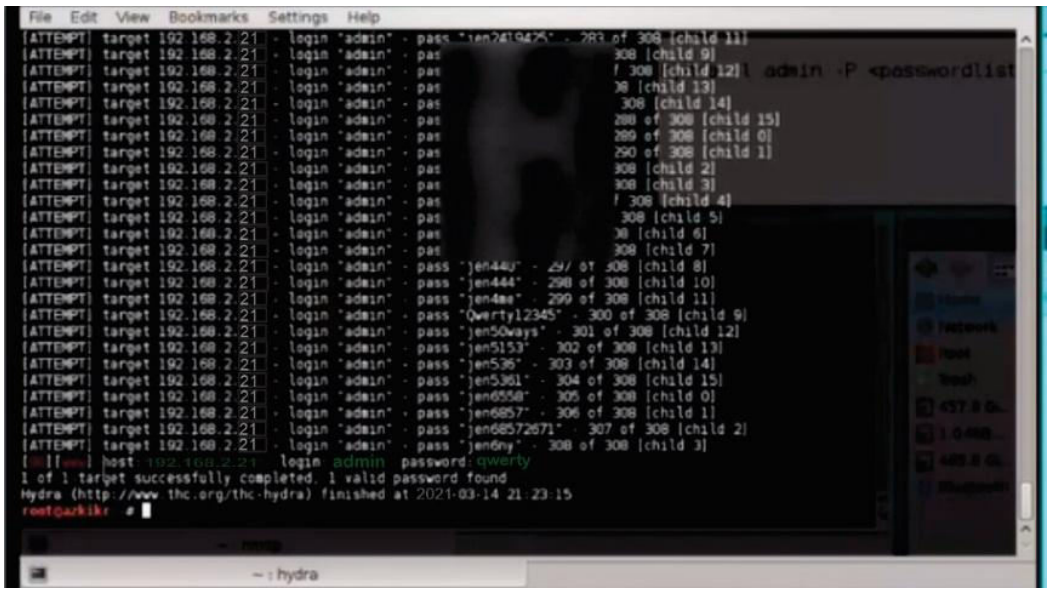



**Gambar 5.**Hasil Informasi Port yang di gunakan untuk celah kebocoran

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 aplikasion 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 penestration test mengunakan tool hydra yang dilakukan mengetikkan 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.

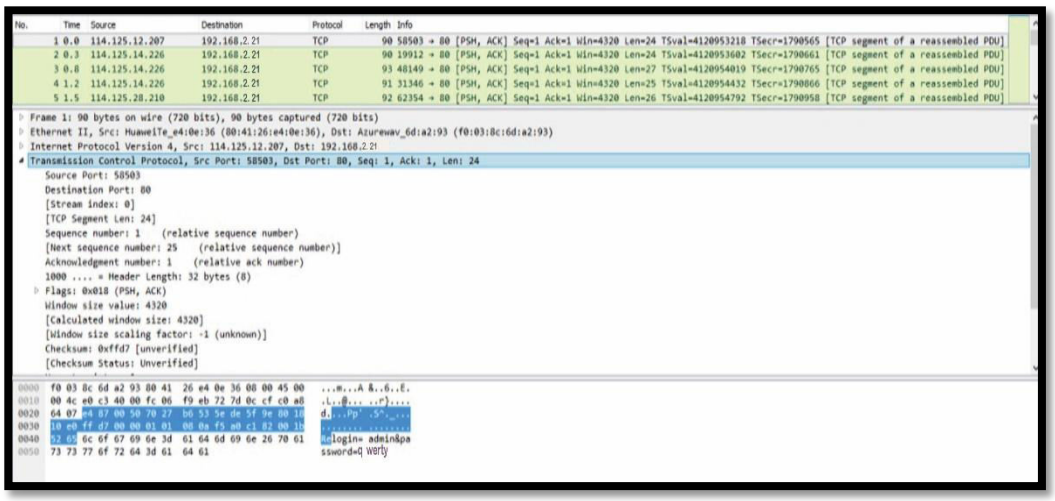



**Gambar 6.** Hasil Penestration Password CCTV target

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***

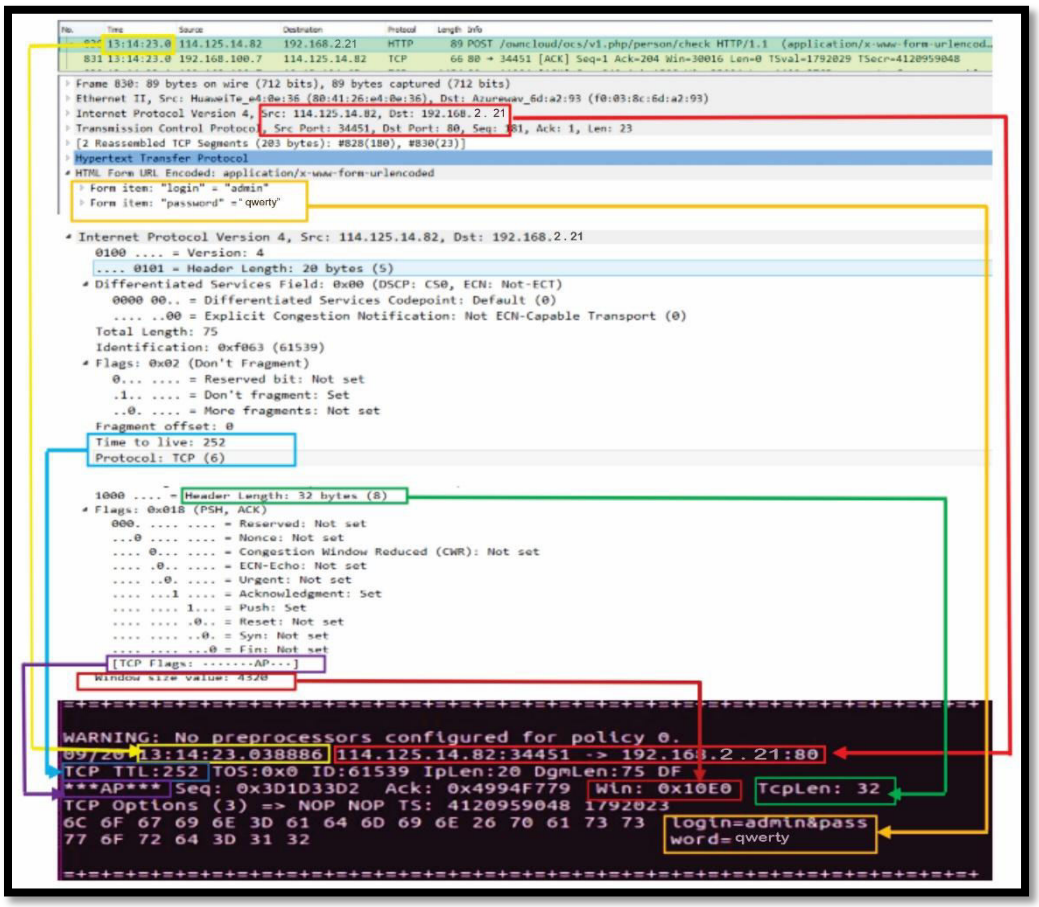
*Wireshark* yaitu *Network Protocol Analyzer*, termasuk juga kedalam satu diantara *network analysis tool atau packet sniffer*. *Wireshark* disini digunakan sebagai mengamati data dari jaringan yang tengah beroperasi (*capturetraffic*)atau dari data yang ada di disk, dan segera melihat atau mensortir 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 *comman separted 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 ata 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.



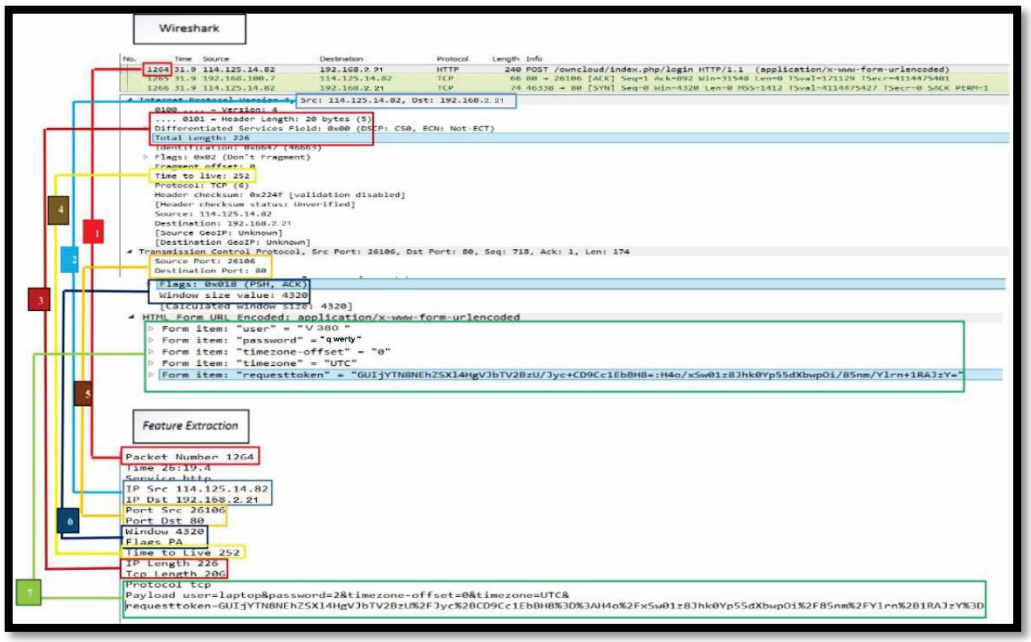

**Gambar 8**. Hasil Analisa *Exploid CCTV* Di Jaringan

### *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 emapt (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 bernilaikan 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. Payloadberisi *user* = laptop, *password* = 2, *timezone-offset* = 0, *timezone*= UTC, dan *requesttoken*=GUIjYTN8NEhZSXl4HgVJbTV2BzU%2FJyc%2BCD9Cc1EbBH8%3D%3AH4o%2FxSw01z8Jhk0Yp55dXbwpOi%2F85nm%2FYlrn%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, 35493, 43025, 50555 | 226, 218, 214, 216, 942, 950, 113, 768 | 206, 198, 194,196, 922, 930,93, 748 |

Pada tabel 1 dan 2 disimpulkan pola akses normal dari skenario pengujianmemiliki 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 fiturdengan 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 diguanakan untuk keperluan mendatang misalnya tujuan keamanan seperti backdoor yang mungkin bisa diekploitasi, maka dibutuhkan penangan 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, "PENGGUNAAN 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.