ANALISIS AKSES PENGGUNA INTERNET MENGGUNAKAN MIKROTIK ROUTER PADA PT. INFORMATION TECHNOLOGY SERVICE CENTRE YOGYAKARTA

Skripsi

Untuk Memenuhi Sebagian Persyaratan

Mencapai Derajat Sarjana S-1

Program Studi Teknik Informatika

Disusun Oleh:

Nugroho Febriansyah Putra

09651006

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2016

Universitas Islam Negeri Sunan Kalijaga **FM-UINSK-BM-05-07/R0**

PENGESAHAN SKRIPSI/TUGAS AKHIR

Nomor : UIN.02/D.ST/PP.01.1/2918/2016

Skripsi/Tugas Akhir dengan judul	:	Analisis Akses Pengguna Internet Menggunakan Mikrotik Router Pada PT. Information Technology Service Centre Yogyakarta
Yang dipersiapkan dan disusun oleh	:	
Nama	:	Nugroho Febriansyah Putra
NIM	:	09651006
Telah dimunaqasyahkan pada	:	Jum'at, 19 Agustus 2016
Nilai Munaqasyah	:	A / B

Dan dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga

TIM MUNAQASYAH :

Ketua Sidang

Sumarsono, M.Kom
NIP. 19710209 200501 1 003

Penguji I

Dr. Bambang Sugiantoro, M.T
NIP.19751024 200912 1 002

Penguji II

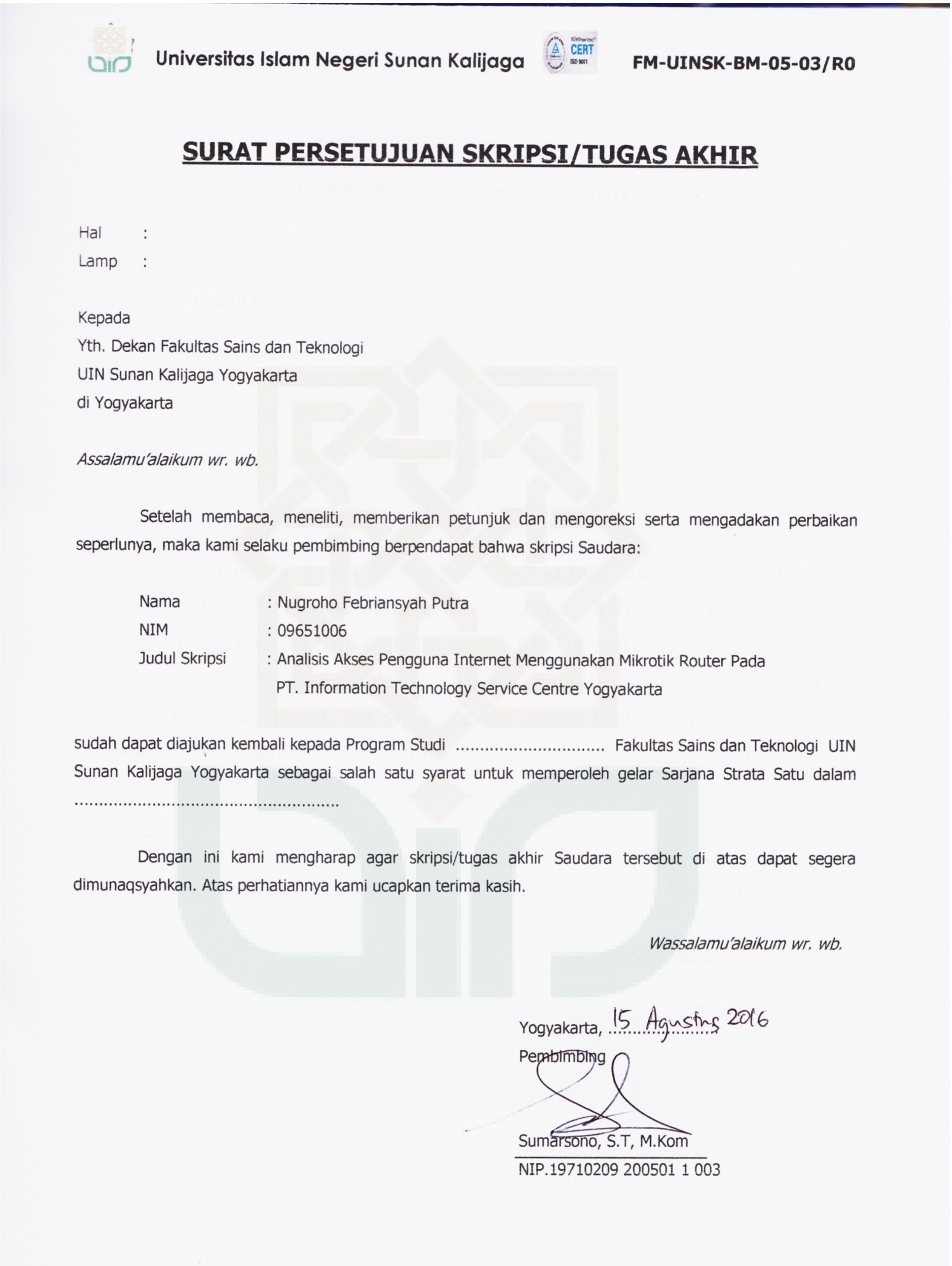
Wahyudi

M. Didik R Wahyudi, M.T
NIP. 19760812 200901 1 015

Yogyakarta, 24 Agustus 2016
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

KEMENTERIAN AGAMA
UIN SUNAN KALIJAGA
YOGYAKARTA
FAKULTAS SAINS DAN TEKNOLOGI
REPUBLIK INDONESIA

Dr. Murtono, M.Si.
NIP. 19691212 200003 1 001



Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-03/R0

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal :
Lamp :

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama	: Nugroho Febriansyah Putra
NIM	: 09651006
Judul Skripsi	: Analisis Akses Pengguna Internet Menggunakan Mikrotik Router Pada PT. Information Technology Service Centre Yogyakarta

sudah dapat diajukan kembali kepada Program Studi .... Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam ....

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqsyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 15 Agustus 2016
Pembimbing

Sumarsono, S.T, M.Kom
NIP.19710209 200501 1 003

PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini:

Nama	: Nugroho Febrinsyah Putra
NIM	: 09651006
Program Studi	: Teknik Informatika
Fakultas	: Sains dan Teknologi

Menyatakan bahwa skripsi dengan judul **"ANALISIS AKSES PENGGUNA INTERNET MENGGUNAKAN MIKROTIK ROUTER PADA PT. INFORMATION TECHNOLOGY SERVICE CENTRE YOGYAKARTA"** tidak terdapat pada karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu Perguruan Tinggi, dan sepengetahuan penulis tidak terdapat karya atau pendapat yang pernah ditulis oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta,15 Agustus 2016

Yang menyatakan

METERAI TEMPEL
TGL
394FCADF608035276
6000
ENAM RIBU RUPIAH

Nugroho Febriansyah Putra
NIM : 09651006

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Assalamu'alaikum Wr. Wb

Alhamdulillahirobbil'alamin, puji syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan rahmat, hidayah, dan inayah-Nya, sehingga dapat menyelesaikan penulisan skripsi ini. Adapun tujuan dari penulisan skripsi ini adalah untuk memenuhi salah satu syarat untuk menyelesaikan program studi Strata Satu (S1), Jurusan Teknik Informatika di Universitas Islam Negeri Sunan Kalijaga Yogyakarta.

Penyusunan skripsi ini tidak terlepas dari bimbingan, pengarahan, bantuan dan dukungan dari berbagai pihak baik secara materiil maupun spiritual. Untuk itu perkenankanlah dalam kesempatan ini penulis mengucapkan terima kasih kepada:

1. Kedua orang tua tercinta dan sodariku tersayang yang senantiasa selalu memberikan doa, dukungan, perhatian dan pengorbanan yang begitu besar. Semoga selalu dalam keridhoan dan lindungan Allah SWT, Amin.
2. Prof. Dr. KH. Yudian Wahyudi, P.hD, selaku Rektor Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
3. Dr. Murtono, M.Si, selaku dekan Fakultas Sains dan Teknologi.
4. Sumarsono, S.T, M.Kom, selaku ketua Program Studi Teknik Informatika dan selaku Dosen Pembimbing yang telah memberikan bimbingan arahan kepada penulis selama penyusunan skripsi ini.
5. Shofwatul 'Uyun, M.Kom, selaku Dosen Pembimbing Akademik.

6. Teman-teman seperjuangan Teknik Informatika Mandiri & Reguler 2009 dan angkatan sebelum dan sesudahnya.
7. Tim KKN UIN Sunan Kalijaga Yogyakarta angkatan ke-77, khususnya kelompok Monggol 1, 2, dan 3 (Cak Ngandhiem, Caki, Bob, Fiki, Nita, Wahyu, dan kawan-kawan).
8. Semua pihak yang telah membantu dalam penyusunan skripsi ini yang tidak dapat disebutkan satu persatu. Terima kasih semua.

Dalam penulisan skripsi ini penulis menyadari masih terdapat kekurangan-kekurangan untuk itu kritik dan saran yang bersifat membangun selalu diharapkan demi kesempurnaan skripsi ini. Penulis juga berharap semoga skripsi ini dapat memberikan manfaat bagi penulis dan pembaca sekalian, dan untuk kemajuan dan perkembangan ilmu pengetahuan.

Wassalamu'alaikum Wr. Wb

Yogyakarta, 15 Agustus 2016

Penyusun

Nugroho Febriansyah Putra
NIM. 09651006

HALAMAN PERSEMBAHAN

Dengan mengucap syukur Alhamdulillah skripsi ini penulis persembahkan untuk:

- Ibunda dan Ayahanda tercinta dan Saudari tersayang yang senantiasa selalu memberikan segala doa, ridho, perhatian, kasih sayang, pengorbanan dan dukungan yang begitu besar dalam hidupku.
- Segenap keluarga besar di Jogja, terima kasih atas doa dan dukungannya selama ini.
- Teman-teman Teknik Informatika Khusus 2009 terimakasih untuk kebersamaan & kekompakannya, Rofitri, Sigit Kiand, Wahyu R, Izza, Wahyu Std, Fiki, Anas, M. Rifai, Agung, Rinanda, Navi, Ainir, Tata, Via. Eka. Kalian LuarBiasa.!!
- Seluruh dosen, staff, civitas akademika Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
- Semua sahabat Maiyah Mocopat Syafaat terimakasih atas waktunya untuk menemani ngopi, begadang, diskusi, berbagi ide dan pengalaman.
- Semua takmir dan jamaah Masjid Jenderal Sudirman Kompleks Colombo Gejayan.
- Semua teman, rekan, relasi, dan pihak yang telah banyak membantu dalam penyusunan skripsi ini yang tidak dapat disebutkan satu persatu.
- Para pembaca laporan skripsi ini, terimakasih telah menyempatkan waktu membaca laporan ini, semoga bermanfaat dan dapat menambah ilmu.

TerimaKasih.

HALAMAN MOTTO

"Tiada Tuhan selain Allah SWT, dan Nabi Muhammad SAW adalah utusan Allah"

"Hidup yang tidak diuji adalah kehidupan yang tidak berharga" Socrates.

"Man makes his own history" Marx

"Pengetahuan, kecerdasan, dan kepintaran adalah seksi yang baru. Ia bahkan mengalahkan ide seksi yang di standart-kan menurut kemolekan tubuh dan ukuran besar payudara" Afi.

"Apa gunanya ilmu jika tidak memperluas jiwa seseorang, sehingga ia berlaku seperti samudra yang menampung sampah-sampah? Apa gunanya kepandaian jika tidak memperbesar kepribadian manusia, sehingga ia makin sanggup memahami orang lain?" Markesot

"Siapkan untuk kalah, sebab kesiapan untuk menang sudah dikerjakan oleh naluri, tak usah anda rancang. Amat susah untuk kalah, menang itu gampang" Markesot

"Kemungkinan terbesar sekarang adalah memperbesar kemungkinan pada ruang ketidak-mungkinan sehingga setiap orang yang kami temui tak menemukan lagi satupun sudut kemungkinan untuk berkata tidak mungkin tanpa darah mereka mengering sebelum mata pena berkarat menolak kembali terisi sebelum semua paru disesaki tragedi dan pengulangan menemukan maknanya sendiri" Morgue Vanguard

"Teralienasi, terhakimi. Kalian bukan mereka, Era baru, milik kalian, hapus norma usang. Tampak beda, tak meyakinkan? Hanya sisi luar saja. Kau serigala, yang teredam, cukup sudah kau terinjak. Buka pikiranmu [luaskan sudut pandang]. Lelah dengan perlakuan dunia, saat unjuk taring. Mereka tak mengerti [serigala]. Kau tidak sendiri [militia]. Lewati jalan nya hari ini. Lewati jalan, tetap impresif. Ayo. Kita taklukan" Seringai – serigala militia

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

Analisis Akses Pengguna Internet Menggunakan Mikrotik Router Pada PT. Information Technology Service Centre Yogyakarta

Nugroho Febriansyah Putra
NIM. 09651006

INTISARI

Di PT. Information Technology Service Centre Yogyakarta dalam penggunaan jaringan internet sangatlah dibutuhkan, hal tersebut disebabkan oleh derasnya arus globalisasi demi layanan informasi yang sangat tinggi agar menghemat waktu kerja dan menginginkan langkah praktis. Kecurangan dalam hal pengaksesan suatu informasi yang menyebabkan turunnya kinerja para pegawai dan terganggunya jalur akses internet sangatlah merugikan bagi perusahaan.

Metode analisis akses pengguna internet dengan *Tool Torch* dan *MT Syslog Daemon* yang disediakan oleh *Mikrotik* berfungsi untuk melihat lalu lintas jaringan apa saja yang melewati router secara *realtime* (pada saat itu) oleh admin, implementasi ini diterapkan pada *router mikrotik* yang sudah terhubung antara *dial up* modem dan *switch hub* sebagai perangkat kerasnya. Metode ini bermanfaat bagi admin untuk meminimalisir terjadi kecurangan dalam setiap akses internet milik perusahaan.

Penggunaan metode analisa akses pengguna internet yaitu dengan melihat akses internet apa saja yang sedang berjalan digunakan untuk menjaga agar koneksi internet tetap berjalan lancar dan meminimalisir kecurangan, namun masih diperlukan konfigurasi manual untuk menjadikan metode ini berjalan lebih optimal. Dari hasil analisa akses pengguna internet pada PT. Information Technology Service Centre Yogyakarta direkomendasikan untuk lebih optimal dalam hal pengawasan setiap pengguna akses internet milik perusahaan.

Kata kunci : Akses Internet, Mikrotik, *Torch*, *MT Syslog Daemon.*

Analysis of User Internet Access Using Mikrotik Router On PT. Information Technology Service Centre Yogyakarta

Nugroho Febriansyah Putra
NIM. 096510006

ABSTRACT

PT. Information Technology Service Centre of Yogyakarta in the use of the internet network is absolutely required, it is caused by the current globalization of the battle for the sake of information services is very high in order to save working time and want practical steps. Cheating in terms of accessing information that caused the decline in the performance of the employees and the disruption of internet access points is very detrimental for the company.

Access analysis method of internet users with Tools Torch and MT Syslog Daemon provided by Mikrotik serves to see any network traffic that passes through the router in realtime (at the time) by the admin, this implementation is implemented on the router mikrotik already connected between a dial-up modem and hub switch as hardware. This method is useful for Admins to minimize cheating occurred in each of the company's internet access.

The use of internet users access to analysis methods, naming by looking at any internet access that is running is used to keep internet connections running smoothly and minimize cheating, but still required manual configuration to make this method run more optimally. From the results of the analysis of users access the internet at PT. Information Technology Service Centre of Yogyakarta is recommended to be optimized in terms of supervision every user of the company's internet access.

Keywords: Internet Access, Mikrotik, Torch, MT Syslog Daemon.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan dunia internet saat ini sangat pesat seiring dengan peningkatan kebutuhan layanan yang cepat dan efisien. Begitu juga dengan komunikasi data, mulai dari koneksi antar dua komputer hingga jaringan komputer. Jaringan komputer saat ini merupakan suatu layanan yang sangat dibutuhkan. Jaringan komputer mempunyai manfaat yang lebih dibandingkan dengan komputer yang berdiri sendiri. Jaringan komputer memungkinkan pemakaian berbagi secara bersama baik dalam data, perangkat lunak dan peralatan. Sehingga sebuah kelompok kerja dapat berkomunikasi lebih efektif dan efisien.

Tujuan utama penggunaan internet di sebuah perusahaan adalah membantu untuk memudahkan kinerja pegawai namun pegawai cenderung lebih banyak menggunakan internet untuk kegiatan bersifat kurang mendukung pekerjaan. Kebebasan akses penggunaan internet terbukti dapat menimbulkan dampak negative. Materi game terlebih pada situs jejaring facebook sangatlah mudah diakses lewat pemanfaatan internet. Kasus ini sudah sering ditemukan di berbagai perusahaan dan tidak menutup kemungkinan terjadi di PT. ITSC Yogyakarta. Kekhawatiran mudahnya mengakses situs tersebut, ditambah dengan munculnya jejaring sosial lain yang sekarang sangat digemari oleh banyak orang. Apabila penggunaanya pada jam-jam kerja sering mengganggu kinerja pegawai, sehingga lupa untuk menyelesaikan pekerjaan, menunda pekerjaan, dan lain sebagainya sehingga menjadi tidak sehat.

MikroTik Router Board adalah sebuah perangkat keras yang sengaja di buat untuk menjalankan router OS mikrotik. Ketika membeli sebuah Mikrotik Router Board biasanya sudah terinstal Router OS didalamnya. Mikrotik Router Board dapat digunakan sebagai router jaringan yang handal, mencakup berbagai fitur lengkap untuk mengelola sebuah jaringan komputer. Selain itu MikroTik dapat juga berfungsi sebagai firewall filter bagi akses pengguna dan memberikan prioritas bagi akses pengguna lain agar bisa mengakses Internet. MikroTik bertujuan untuk melihat, mengawasi dan memonitoring lalu lintas internet yang sedang berlangsung. Penempatan router MikroTik berada diantara modem dan hub yang dijadikan sebagai *gateway* suatu jaringan. Mikrotik *gateway* tersebut berfungsi untuk mendistribusikan data keluar masuknya internet dari dan ke jaringan lainnya sehingga seluruh akses pengguna komputer yang mengakses internet yang melewati mikrotik dapat terlihat.

Dari analisis diatas dapat ditarik kesimpulan bahwa pengelolaan jaringan merupakan salah satu alternatif penyelesaian masalah supaya didapatkan layanan kinerja yang efisien dan maksimal. Dengan adanya Mikrotik Router sebagai *gateway* untuk memonitoring lalu lintas akses internet semoga segala aktivitas pengguna yang diperoleh ke depan dapat membantu permasalahan yang ada.

1.2 Rumusan Masalah

Dari uraian latar belakang masalah yang telah dijabarkan di atas maka penulis merumuskan pokok masalah yang akan di teliti adalah bagaimana cara menganalisa akses lalu lintas internet pada sebuah jaringan internet menggunakan MikroTik Router lalu dengan hasil yang di peroleh dapat membantu pemanfaatan jaringan internet yang ada secara bijak sesuai aturan yang telah disepakati bersama.

1.3 Batasan Masalah

Dalam penyusunan skripsi ini penyusun memberikan batasan masalah agar dalam penjelasannya nanti akan lebih terarah, dan sesuai dengan yang diharapkan. Adapun batasan masalah yang dibahas adalah :

1) Penelitian difokuskan pada jaringan kantor PT. ITSC Yogyakarta.
2) Alat yang digunakan Mikrotik Rb 750r2 yang sudah terinstall Mikrotik Router OS sebagai firewall dan proxy log.
3) Konfigurasi Mikrotik menggunakan winbox.
4) Jumlah akses pengguna 4 orang pegawai yang akan dianalisa.
5) Fokus analisa yang akan di periksa saat user melakukan browsing yaitu protokol, source address (sumber alamat), source port (sumber port), destination address (tujuan alamat), destination port (tujuan port), transmmites rate.
6) Untuk menampilkan hasil analisa akses internet menggunakan remote dengan aplikasi MT Syslog Daemon yang telah disediakan Mikrotik.

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah untuk menganalisa lalu lintas akses pengguna internet yang sedang berlangsung di PT. Information Technology Service Centre Yogyakarta.

1.5 Manfaat Penelitian

Dengan diadakannya penelitian ini, diharapkan data hasil analisis dapat memberikan informasi, pengetahuan dan pemahaman sebagai nantinya dapat menjadi rekomendasi administrator terkait kinerja pegawai saat mengakses internet.

1.6 Keaslian Penelitian

Pada Universitas Islam Negri Sunan Kalijaga Yogyakarta, sudah pernah dilakukan penelitian tentang Mikrotik, akan tetapi untuk masalah mengenai penelitian yang menitik beratkan tentang Analisis Akses Pengguna Internet Menggunakan Mikrotik Router belum pernah dilakukan.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari penelitian berupa analisis akses pengguna internet menggunakan mikrotik pada PT. Information Technology Service Centre Yogyakarta yang telah dilakukan dapat disimpulkan bahwa : Dari sejumlah empat orang pengguna yang di analisa, dua orang pengguna melakukan akses internet secara normal sesuai dengan kebijakan dari perusahaan, sedangkan dua diantaranya melalukan kecurangan dalam akses penggunaan internet, seperti melakukan download dan streaming video berisi konten hiburan pada saat jam kerja.

5.2 Saran

Beberapa saran yang dapat dipertimbangkan :

1. Karena jaringan ini masih menggunakan jaringan skala kecil, maka hasil yang didapat masih kurang maksimal. Diharapkan kepada peneliti selanjutnya untuk pengembangkan metode analisa dengan perbandingan metode logging yang lainnya menggunakan jaringan yang lebih besar.
2. Semoga kedepan dapat di tambahkan proxy server Intrusion Detection System agar saat monitoring akses para pengguna dapat berjalan lebih maksimal.
3. Perlu dilakukannya pemblokiran situs tertentu atau dijadwalkan agar di saat jam kerja bisa lebih optimal dan saat jam istirahat semua akses dibuka.

DAFTAR PUSTAKA

Kustanto, Daniel. 2008. *Membangun Server Internet Dengan Mikrotik OS*, Gava Media Yogyakarta.

Gatra, Ramadhan. 2009. *Manajemen Jaringan Menggunakan Mikrotik*. Skripsi. UIN Sunan Kalijaga Yogyakarta

Anis Rifai, Arfan. 2011. *Analisis dan Implementasi Quality Of Service Pada Router OS Mikrotik*. Skripsi. UIN Sunan Kalijaga Yogyakarta

Nur Hayati, Siti. 2012. *Analisis Bandwidth Management Menggunakan Mikrotik*. Skripsi. UIN Sunan Kalijaga Yogyakarta

Rahmawan, Agung. 2013. *Analisis Perbandingan Metode Load Balancing Peer Connection Classifier (PCC) Dengan NTH Pada Router Mikrotik*. Skripsi. UIN Sunan Kalijaga Yogyakarta

mikrotik.co.id/getfile.php?nf=MT_Syslog.exe 5 April 2016

http://melwin-ok.com/2014/02/ppdioo/ diakses 10 Juli 2016

http://www.ciscozine.com/the-ppdioo-network-lifecycle/ diakses 10 Juli 2016

http://www.ciscopress.com/articles/article.asp?p=1608131&seqNum=3 diakses 10 Juli 2016

http://www.mikrotik.com/archive.php diakses 10 Juli 2016

http://www.forummikrotik.com/scripting-@-mikrotik/10799-cara-menggunakan-syslog-daemon-mikrotik.html diakses 10 Juli 2016

http://www.mikrotik.co.id (memuat tentang perintah dasar mikrotikOS dan referensi mengenai networking mikrotikOS)

LAMPIRAN

Lampiran 1

Analisis Akses Pengguna Tanggal 12 Agustus 2016 Pukul 17.00-18.00Wib

```
system,info log rule changed by admin in 12-Aug 17:6:16.63 from
192.168.88.1
system,info log rule changed by admin in 12-Aug 17:6:17.97 from
192.168.88.1
dns,packet --- got query from 192.168.66.20:63451: in 12-Aug
17:6:50.98 from 192.168.88.1
dns,packet id:6977 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
12-Aug 17:6:50.99 from 192.168.88.1
dns,packet question: ssl.gstatic.com:A:IN in 12-Aug 17:6:50.99
from 192.168.88.1
dns query from 192.168.66.20: #1854 ssl.gstatic.com. A in 12-Aug
17:6:50.99 from 192.168.88.1
dns,packet --- sending udp query to 8.8.4.4:53: in 12-Aug
17:6:50.99 from 192.168.88.1
dns,packet id:9773 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
12-Aug 17:6:51.0 from 192.168.88.1
dns,packet question: ssl.gstatic.com:A:IN in 12-Aug 17:6:51.0
from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:37167->8.8.4.4:53, len 61 in 12-Aug 17:6:51.0 from
192.168.88.1
dns,packet --- got answer from 8.8.4.4:53: in 12-Aug 17:6:51.0
from 192.168.88.1
dns,packet id:9773 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
12-Aug 17:6:51.1 from 192.168.88.1
dns,packet question: ssl.gstatic.com:A:IN in 12-Aug 17:6:51.1
from 192.168.88.1
dns,packet answer: in 12-Aug 17:6:51.1 from 192.168.88.1
dns,packet <ssl.gstatic.com:A:272=74.125.68.94> in 12-Aug
17:6:51.1 from 192.168.88.1
dns,packet <ssl.gstatic.com:A:272=74.125.68.120> in 12-Aug
17:6:51.2 from 192.168.88.1
dns done query: #1854 ssl.gstatic.com 74.125.68.94 in 12-Aug
17:6:51.2 from 192.168.88.1
dns,packet --- sending reply to 192.168.66.20:63451: in 12-Aug
17:6:51.2 from 192.168.88.1
dns,packet id:6977 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
12-Aug 17:6:51.2 from 192.168.88.1
dns,packet question: ssl.gstatic.com:A:IN in 12-Aug 17:6:51.3
from 192.168.88.1
dns,packet answer: in 12-Aug 17:6:51.3 from 192.168.88.1
dns,packet <ssl.gstatic.com:A:272=74.125.68.94> in 12-Aug
17:6:51.5 from 192.168.88.1
dns,packet <ssl.gstatic.com:A:272=74.125.68.120> in 12-Aug
17:6:51.5 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto UDP, 192.168.66.20:63452-
```

```
>74.125.68.94:443, len 1378 in 12-Aug 17:6:51.5 from
192.168.88.1
dns,packet --- got query from 192.168.66.20:60918: in 12-Aug
17:7:27.75 from 192.168.88.1
dns,packet id:f31f rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
12-Aug 17:7:27.75 from 192.168.88.1
dns,packet question: s.youtube.com:A:IN in 12-Aug 17:7:27.75
from 192.168.88.1
dns query from 192.168.66.20: #1855 s.youtube.com. A in 12-Aug
17:7:27.76 from 192.168.88.1
dns,packet --- sending udp query to 8.8.4.4:53: in 12-Aug
17:7:27.76 from 192.168.88.1
dns,packet id:a344 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
12-Aug 17:7:27.76 from 192.168.88.1
dns,packet question: s.youtube.com:A:IN in 12-Aug 17:7:27.76
from 192.168.88.1
dns,packet --- got answer from 8.8.4.4:53: in 12-Aug 17:7:27.84
from 192.168.88.1
dns,packet id:a344 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
12-Aug 17:7:27.84 from 192.168.88.1
dns,packet question: s.youtube.com:A:IN in 12-Aug 17:7:27.84
from 192.168.88.1
dns,packet answer: in 12-Aug 17:7:27.85 from 192.168.88.1
dns,packet <s.youtube.com:CNAME:3136=video-stats.l.google.com>
in 12-Aug 17:7:27.85 from 192.168.88.1
dns,packet <video-stats.l.google.com:A:251=74.125.200.113> in
12-Aug 17:7:27.85 from 192.168.88.1
dns,packet <video-stats.l.google.com:A:251=74.125.200.102> in
12-Aug 17:7:27.85 from 192.168.88.1
dns,packet <video-stats.l.google.com:A:251=74.125.200.100> in
12-Aug 17:7:27.85 from 192.168.88.1
dns,packet <video-stats.l.google.com:A:251=74.125.200.139> in
12-Aug 17:7:27.85 from 192.168.88.1
dns,packet <video-stats.l.google.com:A:251=74.125.200.101> in
12-Aug 17:7:27.86 from 192.168.88.1
dns,packet <video-stats.l.google.com:A:251=74.125.200.138> in
12-Aug 17:7:27.87 from 192.168.88.1
dns done query: #1855 s.youtube.com 74.125.200.113 in 12-Aug
17:7:27.88 from 192.168.88.1
dns,packet --- sending reply to 192.168.66.20:60918: in 12-Aug
17:7:27.88 from 192.168.88.1
dns,packet id:f31f rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
12-Aug 17:7:27.89 from 192.168.88.1
dns,packet question: s.youtube.com:A:IN in 12-Aug 17:7:27.89
from 192.168.88.1
dns,packet answer: in 12-Aug 17:7:27.90 from 192.168.88.1
dns,packet <s.youtube.com:CNAME:3136=video-stats.l.google.com>
in 12-Aug 17:7:27.91 from 192.168.88.1
dns,packet <video-stats.l.google.com:A:251=74.125.200.113> in
12-Aug 17:7:27.92 from 192.168.88.1
dns,packet <video-stats.l.google.com:A:251=74.125.200.102> in
12-Aug 17:7:27.92 from 192.168.88.1
dns,packet <video-stats.l.google.com:A:251=74.125.200.100> in
12-Aug 17:7:27.93 from 192.168.88.1
dns,packet <video-stats.l.google.com:A:251=74.125.200.139> in
12-Aug 17:7:27.94 from 192.168.88.1
```

```
dns,packet <video-stats.l.google.com:A:251=74.125.200.101> in
12-Aug 17:7:27.95 from 192.168.88.1
dns,packet <video-stats.l.google.com:A:251=74.125.200.138> in
12-Aug 17:7:27.95 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:37041->8.8.4.4:53, len 59 in 12-Aug 17:7:27.96
from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto UDP, 192.168.66.20:60919-
>74.125.200.113:443, len 1378 in 12-Aug 17:7:27.97 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:54193-
>74.125.200.113:443, len 52 in 12-Aug 17:7:28.16 from
192.168.88.1
dns,packet --- got query from 192.168.66.20:63747: in 12-Aug
17:7:43.29 from 192.168.88.1
dns,packet id:3a60 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
12-Aug 17:7:43.30 from 192.168.88.1
dns,packet question: www.youtube.com:A:IN in 12-Aug 17:7:43.30
from 192.168.88.1
dns query from 192.168.66.20: #1856 www.youtube.com. A in 12-Aug
17:7:43.32 from 192.168.88.1
dns,packet --- sending udp query to 8.8.4.4:53: in 12-Aug
17:7:43.34 from 192.168.88.1
dns,packet id:dcad rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
12-Aug 17:7:43.35 from 192.168.88.1
dns,packet question: www.youtube.com:A:IN in 12-Aug 17:7:43.36
from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:36770->8.8.4.4:53, len 61 in 12-Aug 17:7:43.39
from 192.168.88.1
dns,packet --- got answer from 8.8.4.4:53: in 12-Aug 17:7:43.45
from 192.168.88.1
dns,packet id:dcad rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
12-Aug 17:7:43.45 from 192.168.88.1
dns,packet question: www.youtube.com:A:IN in 12-Aug 17:7:43.46
from 192.168.88.1
dns,packet answer: in 12-Aug 17:7:43.47 from 192.168.88.1
dns,packet <www.youtube.com:CNAME:85062=youtube-ui.l.google.com>
in 12-Aug 17:7:43.47 from 192.168.88.1
dns,packet <youtube-ui.l.google.com:A:278=74.125.200.91> in 12-
Aug 17:7:43.48 from 192.168.88.1
dns,packet <youtube-ui.l.google.com:A:278=74.125.200.93> in 12-
Aug 17:7:43.49 from 192.168.88.1
dns,packet <youtube-ui.l.google.com:A:278=74.125.200.190> in 12-
Aug 17:7:43.49 from 192.168.88.1
dns,packet <youtube-ui.l.google.com:A:278=74.125.200.136> in 12-
Aug 17:7:43.50 from 192.168.88.1
dns done query: #1856 www.youtube.com 74.125.200.91 in 12-Aug
17:7:43.52 from 192.168.88.1
dns,packet --- sending reply to 192.168.66.20:63747: in 12-Aug
17:7:43.53 from 192.168.88.1
dns,packet id:3a60 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
12-Aug 17:7:43.54 from 192.168.88.1
dns,packet question: www.youtube.com:A:IN in 12-Aug 17:7:43.55
```

```
from 192.168.88.1
dns,packet answer: in 12-Aug 17:7:43.56 from 192.168.88.1
dns,packet <www.youtube.com:CNAME:85063=youtube-ui.l.google.com>
in 12-Aug 17:7:43.56 from 192.168.88.1
dns,packet <youtube-ui.l.google.com:A:278=74.125.200.91> in 12-
Aug 17:7:43.57 from 192.168.88.1
dns,packet <youtube-ui.l.google.com:A:278=74.125.200.93> in 12-
Aug 17:7:43.58 from 192.168.88.1
dns,packet <youtube-ui.l.google.com:A:278=74.125.200.190> in 12-
Aug 17:7:43.58 from 192.168.88.1
dns,packet <youtube-ui.l.google.com:A:278=74.125.200.136> in 12-
Aug 17:7:43.59 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto UDP, 192.168.66.20:63748-
>74.125.200.91:443, len 1378 in 12-Aug 17:7:43.60 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto UDP, 192.168.66.20:63750-
>74.125.68.94:443, len 1378 in 12-Aug 17:7:51.21 from
192.168.88.1
dns,packet --- got query from 192.168.66.20:61618: in 12-Aug
17:8:45.94 from 192.168.88.1
dns,packet id:f6e rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
12-Aug 17:8:45.95 from 192.168.88.1
dns,packet question: plus.google.com:A:IN in 12-Aug 17:8:45.95
from 192.168.88.1
dns query from 192.168.66.20: #1857 plus.google.com. A in 12-Aug
17:8:45.96 from 192.168.88.1
dns,packet --- sending udp query to 8.8.4.4:53: in 12-Aug
17:8:45.97 from 192.168.88.1
dns,packet id:f456 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
12-Aug 17:8:45.98 from 192.168.88.1
dns,packet question: plus.google.com:A:IN in 12-Aug 17:8:45.98
from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:42413->8.8.4.4:53, len 61 in 12-Aug 17:8:46.3 from
192.168.88.1
dns,packet --- got answer from 8.8.4.4:53: in 12-Aug 17:8:46.4
from 192.168.88.1
dns,packet id:f456 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
12-Aug 17:8:46.4 from 192.168.88.1
dns,packet question: plus.google.com:A:IN in 12-Aug 17:8:46.5
from 192.168.88.1
dns,packet answer: in 12-Aug 17:8:46.6 from 192.168.88.1
dns,packet <plus.google.com:A:269=74.125.200.113> in 12-Aug
17:8:46.6 from 192.168.88.1
dns,packet <plus.google.com:A:269=74.125.200.101> in 12-Aug
17:8:46.7 from 192.168.88.1
dns,packet <plus.google.com:A:269=74.125.200.102> in 12-Aug
17:8:46.8 from 192.168.88.1
dns,packet <plus.google.com:A:269=74.125.200.138> in 12-Aug
17:8:46.8 from 192.168.88.1
dns,packet <plus.google.com:A:269=74.125.200.100> in 12-Aug
17:8:46.9 from 192.168.88.1
dns,packet <plus.google.com:A:269=74.125.200.139> in 12-Aug
17:8:46.10 from 192.168.88.1
```

```
dns done query: #1857 plus.google.com 74.125.200.113 in 12-Aug
17:8:46.10 from 192.168.88.1
dns,packet --- sending reply to 192.168.66.20:61618: in 12-Aug
17:8:46.11 from 192.168.88.1
dns,packet id:f6e rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
12-Aug 17:8:46.12 from 192.168.88.1
dns,packet question: plus.google.com:A:IN in 12-Aug 17:8:46.12
from 192.168.88.1
dns,packet answer: in 12-Aug 17:8:46.13 from 192.168.88.1
dns,packet <plus.google.com:A:269=74.125.200.113> in 12-Aug
17:8:46.14 from 192.168.88.1
dns,packet <plus.google.com:A:269=74.125.200.101> in 12-Aug
17:8:46.14 from 192.168.88.1
dns,packet <plus.google.com:A:269=74.125.200.102> in 12-Aug
17:8:46.15 from 192.168.88.1
dns,packet <plus.google.com:A:269=74.125.200.138> in 12-Aug
17:8:46.16 from 192.168.88.1
dns,packet <plus.google.com:A:269=74.125.200.100> in 12-Aug
17:8:46.17 from 192.168.88.1
dns,packet <plus.google.com:A:269=74.125.200.139> in 12-Aug
17:8:46.18 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto UDP, 192.168.66.20:61619-
>74.125.200.113:443, len 1378 in 12-Aug 17:8:46.18 from
192.168.88.1
dns,packet --- got query from 192.168.66.20:50183: in 12-Aug
17:8:50.89 from 192.168.88.1
dns,packet id:de95 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
12-Aug 17:8:50.89 from 192.168.88.1
dns,packet question: csi.gstatic.com:A:IN in 12-Aug 17:8:50.90
from 192.168.88.1
dns query from 192.168.66.20: #1858 csi.gstatic.com. A in 12-Aug
17:8:50.91 from 192.168.88.1
dns,packet --- sending udp query to 8.8.4.4:53: in 12-Aug
17:8:50.91 from 192.168.88.1
dns,packet id:42ae rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
12-Aug 17:8:50.92 from 192.168.88.1
dns,packet question: csi.gstatic.com:A:IN in 12-Aug 17:8:50.93
from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:34271->8.8.4.4:53, len 61 in 12-Aug 17:8:50.98
from 192.168.88.1
dns,packet --- got answer from 8.8.4.4:53: in 12-Aug 17:8:51.2
from 192.168.88.1
dns,packet id:42ae rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
12-Aug 17:8:51.3 from 192.168.88.1
dns,packet question: csi.gstatic.com:A:IN in 12-Aug 17:8:51.4
from 192.168.88.1
dns,packet answer: in 12-Aug 17:8:51.4 from 192.168.88.1
dns,packet <csi.gstatic.com:A:239=216.58.212.131> in 12-Aug
17:8:51.5 from 192.168.88.1
dns,packet <csi.gstatic.com:A:239=216.58.212.163> in 12-Aug
17:8:51.6 from 192.168.88.1
dns,packet <csi.gstatic.com:A:239=216.58.212.195> in 12-Aug
17:8:51.7 from 192.168.88.1
dns,packet <csi.gstatic.com:A:239=216.58.212.227> in 12-Aug
```

```
17:8:51.7 from 192.168.88.1
dns,packet <csi.gstatic.com:A:239=172.217.18.131> in 12-Aug
17:8:51.8 from 192.168.88.1
dns,packet <csi.gstatic.com:A:239=216.58.201.163> in 12-Aug
17:8:51.9 from 192.168.88.1
dns,packet <csi.gstatic.com:A:239=216.58.209.99> in 12-Aug
17:8:51.9 from 192.168.88.1
dns,packet <csi.gstatic.com:A:239=216.58.209.131> in 12-Aug
17:8:51.10 from 192.168.88.1
dns done query: #1858 csi.gstatic.com 216.58.212.131 in 12-Aug
17:8:51.11 from 192.168.88.1
dns,packet --- sending reply to 192.168.66.20:50183: in 12-Aug
17:8:51.11 from 192.168.88.1
dns,packet id:de95 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
12-Aug 17:8:51.12 from 192.168.88.1
dns,packet question: csi.gstatic.com:A:IN in 12-Aug 17:8:51.13
from 192.168.88.1
dns,packet answer: in 12-Aug 17:8:51.13 from 192.168.88.1
dns,packet <csi.gstatic.com:A:239=216.58.212.131> in 12-Aug
17:8:51.14 from 192.168.88.1
dns,packet <csi.gstatic.com:A:239=216.58.212.163> in 12-Aug
17:8:51.15 from 192.168.88.1
dns,packet <csi.gstatic.com:A:239=216.58.212.195> in 12-Aug
17:8:51.15 from 192.168.88.1
dns,packet <csi.gstatic.com:A:239=216.58.212.227> in 12-Aug
17:8:51.16 from 192.168.88.1
dns,packet <csi.gstatic.com:A:239=172.217.18.131> in 12-Aug
17:8:51.16 from 192.168.88.1
dns,packet <csi.gstatic.com:A:239=216.58.201.163> in 12-Aug
17:8:51.17 from 192.168.88.1
dns,packet <csi.gstatic.com:A:239=216.58.209.99> in 12-Aug
17:8:51.18 from 192.168.88.1
dns,packet <csi.gstatic.com:A:239=216.58.209.131> in 12-Aug
17:8:51.19 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto UDP, 192.168.66.20:50184-
>216.58.212.131:443, len 1378 in 12-Aug 17:8:51.19 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:54194-
>216.58.212.131:443, len 52 in 12-Aug 17:8:52.73 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:54195-
>216.58.212.131:443, len 52 in 12-Aug 17:8:52.98 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto UDP, 192.168.66.20:50187-
>74.125.68.94:443, len 1378 in 12-Aug 17:9:6.28 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto UDP, 192.168.66.20:50189-
>74.125.200.113:443, len 1378 in 12-Aug 17:9:27.84 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto UDP, 192.168.66.20:50192-
```

```
>74.125.200.113:443, len 1378 in 12-Aug 17:9:46.34 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:54196-
>74.125.200.113:443, len 52 in 12-Aug 17:9:46.47 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (ACK), 192.168.66.20:54195-
>216.58.212.131:443, len 41 in 12-Aug 17:9:48.83 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto UDP, 192.168.66.20:50194-
>216.58.212.131:443, len 1378 in 12-Aug 17:10:0.18 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto UDP, 192.168.66.20:50196-
>74.125.200.139:443, len 1378 in 12-Aug 17:10:34.36 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto UDP, 192.168.66.20:50197-
>74.125.200.91:443, len 1378 in 12-Aug 17:10:34.37 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:54197-
>74.125.200.139:443, len 52 in 12-Aug 17:10:34.66 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto UDP, 192.168.66.20:50199-
>74.125.68.94:443, len 1378 in 12-Aug 17:10:36.5 from
192.168.88.1
dns,packet --- got query from 192.168.66.20:59590: in 12-Aug
17:10:49.19 from 192.168.88.1
dns,packet id:bcf7 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
12-Aug 17:10:49.20 from 192.168.88.1
dns,packet question: i1.ytimg.com:A:IN in 12-Aug 17:10:49.21
from 192.168.88.1
dns query from 192.168.66.20: #1859 i1.ytimg.com. A in 12-Aug
17:10:49.21 from 192.168.88.1
dns done query: #1859 dns name exists, but no appropriate record
in 12-Aug 17:10:49.22 from 192.168.88.1
dns,packet --- sending reply to 192.168.66.20:59590: in 12-Aug
17:10:49.23 from 192.168.88.1
dns,packet id:bcf7 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
12-Aug 17:10:49.24 from 192.168.88.1
dns,packet question: i1.ytimg.com:A:IN in 12-Aug 17:10:49.25
from 192.168.88.1
dns,packet answer: in 12-Aug 17:10:49.25 from 192.168.88.1
dns,packet <i1.ytimg.com:A:2010=74.125.200.102> in 12-Aug
17:10:49.26 from 192.168.88.1
dns,packet <i1.ytimg.com:A:2010=74.125.200.113> in 12-Aug
17:10:49.27 from 192.168.88.1
dns,packet <i1.ytimg.com:A:2010=74.125.200.138> in 12-Aug
17:10:49.27 from 192.168.88.1
dns,packet <i1.ytimg.com:A:2010=74.125.200.139> in 12-Aug
17:10:49.28 from 192.168.88.1
dns,packet <i1.ytimg.com:A:2010=74.125.200.100> in 12-Aug
```

```
17:10:49.29 from 192.168.88.1
dns,packet <i1.ytimg.com:A:2010=74.125.200.101> in 12-Aug
17:10:49.29 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto UDP, 192.168.66.20:59592-
>74.125.200.113:443, len 1378 in 12-Aug 17:10:55.23 from
192.168.88.1
dns,packet --- got query from 192.168.66.20:51366: in 12-Aug
17:10:59.29 from 192.168.88.1
dns,packet id:9644 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
12-Aug 17:10:59.29 from 192.168.88.1
dns,packet question: i9.ytimg.com:A:IN in 12-Aug 17:10:59.30
from 192.168.88.1
dns query from 192.168.66.20: #1860 i9.ytimg.com. A in 12-Aug
17:10:59.31 from 192.168.88.1
dns,packet --- sending udp query to 8.8.4.4:53: in 12-Aug
17:10:59.31 from 192.168.88.1
dns,packet id:de91 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
12-Aug 17:10:59.32 from 192.168.88.1
dns,packet question: i9.ytimg.com:A:IN in 12-Aug 17:10:59.33
from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:46425->8.8.4.4:53, len 58 in 12-Aug 17:10:59.38
from 192.168.88.1
dns,packet --- got answer from 8.8.4.4:53: in 12-Aug 17:10:59.65
from 192.168.88.1
dns,packet id:de91 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
12-Aug 17:10:59.66 from 192.168.88.1
dns,packet question: i9.ytimg.com:A:IN in 12-Aug 17:10:59.67
from 192.168.88.1
dns,packet answer: in 12-Aug 17:10:59.67 from 192.168.88.1
dns,packet <i9.ytimg.com:CNAME:2069=ytimg.l.google.com> in 12-
Aug 17:10:59.68 from 192.168.88.1
dns,packet <ytimg.l.google.com:A:280=74.125.130.101> in 12-Aug
17:10:59.69 from 192.168.88.1
dns,packet <ytimg.l.google.com:A:280=74.125.130.139> in 12-Aug
17:10:59.69 from 192.168.88.1
dns,packet <ytimg.l.google.com:A:280=74.125.130.102> in 12-Aug
17:10:59.70 from 192.168.88.1
dns,packet <ytimg.l.google.com:A:280=74.125.130.100> in 12-Aug
17:10:59.71 from 192.168.88.1
dns,packet <ytimg.l.google.com:A:280=74.125.130.113> in 12-Aug
17:10:59.72 from 192.168.88.1
dns,packet <ytimg.l.google.com:A:280=74.125.130.138> in 12-Aug
17:10:59.73 from 192.168.88.1
dns done query: #1860 i9.ytimg.com 74.125.130.101 in 12-Aug
17:10:59.74 from 192.168.88.1
dns,packet --- sending reply to 192.168.66.20:51366: in 12-Aug
17:10:59.74 from 192.168.88.1
dns,packet id:9644 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
12-Aug 17:10:59.75 from 192.168.88.1
dns,packet question: i9.ytimg.com:A:IN in 12-Aug 17:10:59.76
from 192.168.88.1
dns,packet answer: in 12-Aug 17:10:59.76 from 192.168.88.1
dns,packet <i9.ytimg.com:CNAME:2069=ytimg.l.google.com> in 12-
Aug 17:10:59.77 from 192.168.88.1
```

```
dns,packet <ytimg.l.google.com:A:280=74.125.130.101> in 12-Aug
17:10:59.78 from 192.168.88.1
dns,packet <ytimg.l.google.com:A:280=74.125.130.139> in 12-Aug
17:10:59.78 from 192.168.88.1
dns,packet <ytimg.l.google.com:A:280=74.125.130.102> in 12-Aug
17:10:59.79 from 192.168.88.1
dns,packet <ytimg.l.google.com:A:280=74.125.130.100> in 12-Aug
17:10:59.80 from 192.168.88.1
dns,packet <ytimg.l.google.com:A:280=74.125.130.113> in 12-Aug
17:10:59.80 from 192.168.88.1
dns,packet <ytimg.l.google.com:A:280=74.125.130.138> in 12-Aug
17:10:59.81 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto UDP, 192.168.66.20:51367-
>74.125.130.101:443, len 1378 in 12-Aug 17:10:59.82 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:54198-
>74.125.130.101:443, len 52 in 12-Aug 17:11:0.3 from
192.168.88.1
dns,packet --- got query from 192.168.66.20:54648: in 12-Aug
17:11:1.76 from 192.168.88.1
dns,packet id:751a rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
12-Aug 17:11:1.76 from 192.168.88.1
dns,packet question: clients4.google.com:A:IN in 12-Aug
17:11:1.77 from 192.168.88.1
dns query from 192.168.66.20: #1861 clients4.google.com. A in
12-Aug 17:11:1.78 from 192.168.88.1
dns,packet --- sending udp query to 8.8.4.4:53: in 12-Aug
17:11:1.78 from 192.168.88.1
dns,packet id:3054 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
12-Aug 17:11:1.79 from 192.168.88.1
dns,packet question: clients4.google.com:A:IN in 12-Aug
17:11:1.80 from 192.168.88.1
dns,packet --- got answer from 8.8.4.4:53: in 12-Aug 17:11:1.80
from 192.168.88.1
dns,packet id:3054 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
12-Aug 17:11:1.81 from 192.168.88.1
dns,packet question: clients4.google.com:A:IN in 12-Aug
17:11:1.82 from 192.168.88.1
dns,packet answer: in 12-Aug 17:11:1.83 from 192.168.88.1
dns,packet <clients4.google.com:CNAME:254=clients.l.google.com>
in 12-Aug 17:11:1.84 from 192.168.88.1
dns,packet <clients.l.google.com:A:265=74.125.200.101> in 12-Aug
17:11:1.84 from 192.168.88.1
dns,packet <clients.l.google.com:A:265=74.125.200.102> in 12-Aug
17:11:1.85 from 192.168.88.1
dns,packet <clients.l.google.com:A:265=74.125.200.139> in 12-Aug
17:11:1.86 from 192.168.88.1
dns,packet <clients.l.google.com:A:265=74.125.200.138> in 12-Aug
17:11:1.87 from 192.168.88.1
dns,packet <clients.l.google.com:A:265=74.125.200.100> in 12-Aug
17:11:1.87 from 192.168.88.1
dns,packet <clients.l.google.com:A:265=74.125.200.113> in 12-Aug
17:11:1.88 from 192.168.88.1
dns done query: #1861 clients4.google.com 74.125.200.101 in 12-
```

```
Aug 17:11:1.89 from 192.168.88.1
dns,packet --- sending reply to 192.168.66.20:54648: in 12-Aug
17:11:1.90 from 192.168.88.1
dns,packet id:751a rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
12-Aug 17:11:1.90 from 192.168.88.1
dns,packet question: clients4.google.com:A:IN in 12-Aug
17:11:1.91 from 192.168.88.1
dns,packet answer: in 12-Aug 17:11:1.92 from 192.168.88.1
dns,packet <clients4.google.com:CNAME:254=clients.l.google.com>
in 12-Aug 17:11:1.92 from 192.168.88.1
dns,packet <clients.l.google.com:A:265=74.125.200.101> in 12-Aug
17:11:1.93 from 192.168.88.1
dns,packet <clients.l.google.com:A:265=74.125.200.102> in 12-Aug
17:11:1.94 from 192.168.88.1
dns,packet <clients.l.google.com:A:265=74.125.200.139> in 12-Aug
17:11:1.95 from 192.168.88.1
dns,packet <clients.l.google.com:A:265=74.125.200.138> in 12-Aug
17:11:1.95 from 192.168.88.1
dns,packet <clients.l.google.com:A:265=74.125.200.100> in 12-Aug
17:11:1.96 from 192.168.88.1
dns,packet <clients.l.google.com:A:265=74.125.200.113> in 12-Aug
17:11:1.97 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:58239->8.8.4.4:53, len 65 in 12-Aug 17:11:1.97
from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto UDP, 192.168.66.20:54649-
>74.125.200.101:443, len 1378 in 12-Aug 17:11:1.98 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:54199-
>74.125.200.101:443, len 52 in 12-Aug 17:11:2.6 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto UDP, 192.168.66.20:54651-
>74.125.68.155:443, len 1378 in 12-Aug 17:11:21.21 from
192.168.88.1
dns,packet --- got query from 192.168.66.20:52087: in 12-Aug
17:11:21.76 from 192.168.88.1
dns,packet id:2313 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
12-Aug 17:11:21.77 from 192.168.88.1
dns,packet question: clients1.google.com:A:IN in 12-Aug
17:11:21.77 from 192.168.88.1
dns query from 192.168.66.20: #1862 clients1.google.com. A in
12-Aug 17:11:21.78 from 192.168.88.1
dns,packet --- sending udp query to 8.8.4.4:53: in 12-Aug
17:11:21.79 from 192.168.88.1
dns,packet id:374b rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
12-Aug 17:11:21.79 from 192.168.88.1
dns,packet question: clients1.google.com:A:IN in 12-Aug
17:11:21.80 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:33100->8.8.4.4:53, len 65 in 12-Aug 17:11:21.85
from 192.168.88.1
dns,packet --- got answer from 8.8.4.4:53: in 12-Aug 17:11:21.89
from 192.168.88.1
```

```
dns,packet id:374b rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
12-Aug 17:11:21.89 from 192.168.88.1
dns,packet question: clients1.google.com:A:IN in 12-Aug
17:11:21.90 from 192.168.88.1
dns,packet answer: in 12-Aug 17:11:21.91 from 192.168.88.1
dns,packet <clients1.google.com:CNAME:222=clients.l.google.com>
in 12-Aug 17:11:21.91 from 192.168.88.1
dns,packet <clients.l.google.com:A:296=74.125.200.100> in 12-Aug
17:11:21.92 from 192.168.88.1
dns,packet <clients.l.google.com:A:296=74.125.200.113> in 12-Aug
17:11:21.93 from 192.168.88.1
dns,packet <clients.l.google.com:A:296=74.125.200.138> in 12-Aug
17:11:21.93 from 192.168.88.1
dns,packet <clients.l.google.com:A:296=74.125.200.101> in 12-Aug
17:11:21.94 from 192.168.88.1
dns,packet <clients.l.google.com:A:296=74.125.200.139> in 12-Aug
17:11:21.95 from 192.168.88.1
dns,packet <clients.l.google.com:A:296=74.125.200.102> in 12-Aug
17:11:21.96 from 192.168.88.1
dns done query: #1862 clients1.google.com 74.125.200.139 in 12-
Aug 17:11:21.97 from 192.168.88.1
dns,packet --- sending reply to 192.168.66.20:52087: in 12-Aug
17:11:21.98 from 192.168.88.1
dns,packet id:2313 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
12-Aug 17:11:21.98 from 192.168.88.1
dns,packet question: clients1.google.com:A:IN in 12-Aug
17:11:21.99 from 192.168.88.1
dns,packet answer: in 12-Aug 17:11:22.0 from 192.168.88.1
dns,packet <clients1.google.com:CNAME:222=clients.l.google.com>
in 12-Aug 17:11:22.1 from 192.168.88.1
dns,packet <clients.l.google.com:A:296=74.125.200.139> in 12-Aug
17:11:22.1 from 192.168.88.1
dns,packet <clients.l.google.com:A:296=74.125.200.138> in 12-Aug
17:11:22.2 from 192.168.88.1
dns,packet <clients.l.google.com:A:296=74.125.200.100> in 12-Aug
17:11:22.3 from 192.168.88.1
dns,packet <clients.l.google.com:A:296=74.125.200.113> in 12-Aug
17:11:22.3 from 192.168.88.1
dns,packet <clients.l.google.com:A:296=74.125.200.101> in 12-Aug
17:11:22.4 from 192.168.88.1
dns,packet <clients.l.google.com:A:296=74.125.200.102> in 12-Aug
17:11:22.5 from 192.168.88.1
dns,packet --- got query from 192.168.66.20:64197: in 12-Aug
17:11:26.64 from 192.168.88.1
dns,packet id:331d rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
12-Aug 17:11:26.65 from 192.168.88.1
dns,packet question: docs.google.com:A:IN in 12-Aug 17:11:26.65
from 192.168.88.1
dns query from 192.168.66.20: #1863 docs.google.com. A in 12-Aug
17:11:26.66 from 192.168.88.1
dns,packet --- sending udp query to 8.8.4.4:53: in 12-Aug
17:11:26.67 from 192.168.88.1
dns,packet id:6474 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
12-Aug 17:11:26.67 from 192.168.88.1
dns,packet question: docs.google.com:A:IN in 12-Aug 17:11:26.68
from 192.168.88.1
```

```
dns,packet --- got answer from 8.8.4.4:53: in 12-Aug 17:11:26.73
from 192.168.88.1
dns,packet id:6474 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
12-Aug 17:11:26.74 from 192.168.88.1
dns,packet question: docs.google.com:A:IN in 12-Aug 17:11:26.75
from 192.168.88.1
dns,packet answer: in 12-Aug 17:11:26.76 from 192.168.88.1
dns,packet <docs.google.com:A:267=216.58.221.78> in 12-Aug
17:11:26.76 from 192.168.88.1
dns done query: #1863 docs.google.com 216.58.221.78 in 12-Aug
17:11:26.77 from 192.168.88.1
dns,packet --- sending reply to 192.168.66.20:64197: in 12-Aug
17:11:26.78 from 192.168.88.1
dns,packet id:331d rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
12-Aug 17:11:26.78 from 192.168.88.1
dns,packet question: docs.google.com:A:IN in 12-Aug 17:11:26.79
from 192.168.88.1
dns,packet answer: in 12-Aug 17:11:26.80 from 192.168.88.1
dns,packet <docs.google.com:A:267=216.58.221.78> in 12-Aug
17:11:26.80 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:45079->8.8.4.4:53, len 61 in 12-Aug 17:11:26.81
from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto UDP, 192.168.66.20:64198-
>216.58.221.78:443, len 1378 in 12-Aug 17:11:26.85 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:54200-
>216.58.221.78:443, len 52 in 12-Aug 17:11:26.95 from
192.168.88.1
dns,packet --- got query from 192.168.66.20:64755: in 12-Aug
17:11:31.9 from 192.168.88.1
dns,packet id:a630 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
12-Aug 17:11:31.9 from 192.168.88.1
dns,packet question: apis.google.com:A:IN in 12-Aug 17:11:31.10
from 192.168.88.1
```

LAMPIRAN 2

Analisis Akses Pengguna Tanggal 13 Agustus 2016 Pukul 09.00-16.07Wib

```
dns,packet question: csi.gstatic.com:A:IN in 13-Aug 13:40:59.48
from 192.168.88.1
dns,packet answer: in 13-Aug 13:41:0.16 from 192.168.88.1
dns,packet <csi.gstatic.com:A:238=216.58.212.131> in 13-Aug
13:41:0.16 from 192.168.88.1
dns,packet <csi.gstatic.com:A:238=216.58.212.163> in 13-Aug
13:41:0.16 from 192.168.88.1
dns,packet <csi.gstatic.com:A:238=216.58.212.195> in 13-Aug
13:41:0.16 from 192.168.88.1
dns,packet <csi.gstatic.com:A:238=216.58.212.227> in 13-Aug
13:41:0.16 from 192.168.88.1
dns,packet <csi.gstatic.com:A:238=172.217.18.131> in 13-Aug
```

```
13:41:0.16 from 192.168.88.1
dns,packet <csi.gstatic.com:A:238=216.58.201.163> in 13-Aug
13:41:0.16 from 192.168.88.1
dns,packet <csi.gstatic.com:A:238=216.58.209.99> in 13-Aug
13:41:0.16 from 192.168.88.1
dns,packet <csi.gstatic.com:A:238=216.58.209.131> in 13-Aug
13:41:0.16 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:37853->8.8.8.8:53, len 61 in 13-Aug 13:41:0.16 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto UDP, 192.168.66.20:52026-
>216.58.212.131:443, len 1378 in 13-Aug 13:41:0.16 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:59907-
>216.58.212.131:443, len 52 in 13-Aug 13:41:0.17 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:59908-
>216.58.212.131:443, len 52 in 13-Aug 13:41:0.31 from 192.168.88.1
dns,packet --- got query from 192.168.66.20:53880: in 13-Aug
13:41:12.64 from 192.168.88.1
dns,packet id:6c2e rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 13:41:12.64 from 192.168.88.1
dns,packet question: m.addthis.com:A:IN in 13-Aug 13:41:12.64 from
192.168.88.1
dns query from 192.168.66.20: #3924 m.addthis.com. A in 13-Aug
13:41:12.64 from 192.168.88.1
dns,packet --- sending udp query to 8.8.8.8:53: in 13-Aug
13:41:12.64 from 192.168.88.1
dns,packet id:b508 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 13:41:12.64 from 192.168.88.1
dns,packet question: m.addthis.com:A:IN in 13-Aug 13:41:12.64 from
192.168.88.1
dns,packet --- got answer from 8.8.8.8:53: in 13-Aug 13:41:12.64
from 192.168.88.1
dns,packet id:b508 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 13:41:12.64 from 192.168.88.1
dns,packet question: m.addthis.com:A:IN in 13-Aug 13:41:12.64 from
192.168.88.1
dns,packet answer: in 13-Aug 13:41:12.64 from 192.168.88.1
dns,packet <m.addthis.com:CNAME:280=m.addthisedge.com> in 13-Aug
13:41:12.65 from 192.168.88.1
dns,packet
<m.addthisedge.com:CNAME:27=m.addthisedge.com.cdn.cloudflare.net>
in 13-Aug 13:41:12.65 from 192.168.88.1
dns,packet
<m.addthisedge.com.cdn.cloudflare.net:A:168=104.16.27.235> in 13-
Aug 13:41:12.65 from 192.168.88.1
dns,packet
<m.addthisedge.com.cdn.cloudflare.net:A:168=104.16.26.235> in 13-
Aug 13:41:12.65 from 192.168.88.1
dns,packet
<m.addthisedge.com.cdn.cloudflare.net:A:168=104.16.24.235> in 13-
Aug 13:41:12.65 from 192.168.88.1
dns,packet
```

```
<m.addthisedge.com.cdn.cloudflare.net:A:168=104.16.25.235> in 13-
Aug 13:41:12.65 from 192.168.88.1
dns,packet
<m.addthisedge.com.cdn.cloudflare.net:A:168=104.16.23.235> in 13-
Aug 13:41:12.65 from 192.168.88.1
dns done query: #3924 m.addthis.com 104.16.27.235 in 13-Aug
13:41:12.65 from 192.168.88.1
dns,packet --- sending reply to 192.168.66.20:53880: in 13-Aug
13:41:12.65 from 192.168.88.1
dns,packet id:6c2e rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 13:41:12.65 from 192.168.88.1
dns,packet question: m.addthis.com:A:IN in 13-Aug 13:41:12.65 from
192.168.88.1
dns,packet answer: in 13-Aug 13:41:12.66 from 192.168.88.1
dns,packet <m.addthis.com:CNAME:280=m.addthisedge.com> in 13-Aug
13:41:12.66 from 192.168.88.1
dns,packet
<m.addthisedge.com:CNAME:27=m.addthisedge.com.cdn.cloudflare.net>
in 13-Aug 13:41:12.66 from 192.168.88.1
dns,packet
<m.addthisedge.com.cdn.cloudflare.net:A:168=104.16.27.235> in 13-
Aug 13:41:12.66 from 192.168.88.1
dns,packet
<m.addthisedge.com.cdn.cloudflare.net:A:168=104.16.26.235> in 13-
Aug 13:41:12.66 from 192.168.88.1
dns,packet
<m.addthisedge.com.cdn.cloudflare.net:A:168=104.16.24.235> in 13-
Aug 13:41:12.66 from 192.168.88.1
dns,packet
<m.addthisedge.com.cdn.cloudflare.net:A:168=104.16.25.235> in 13-
Aug 13:41:12.66 from 192.168.88.1
dns,packet
<m.addthisedge.com.cdn.cloudflare.net:A:168=104.16.23.235> in 13-
Aug 13:41:12.67 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:42901->8.8.8.8:53, len 59 in 13-Aug 13:41:12.74 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:59909-
>203.114.72.72:80, len 52 in 13-Aug 13:41:12.75 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:59910-
>104.16.27.235:80, len 52 in 13-Aug 13:41:12.75 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (ACK), 192.168.66.20:59818-
>74.125.200.95:80, len 41 in 13-Aug 13:41:13.72 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (ACK), 192.168.66.20:59820-
>74.125.200.95:80, len 41 in 13-Aug 13:41:13.72 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (ACK), 192.168.66.20:59819-
>74.125.200.95:80, len 41 in 13-Aug 13:41:13.72 from 192.168.88.1
dns,packet --- got query from 192.168.88.11:49344: in 13-Aug
13:41:17.9 from 192.168.88.1
dns,packet id:36d9 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 13:41:17.9 from 192.168.88.1
```

```
dns,packet question: www.facebook.com:A:IN in 13-Aug 13:41:17.9
from 192.168.88.1
dns query from 192.168.88.11: #3925 www.facebook.com. A in 13-Aug
13:41:17.9 from 192.168.88.1
dns,packet --- sending udp query to 8.8.8.8:53: in 13-Aug
13:41:17.9 from 192.168.88.1
dns,packet id:fef rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in 13-
Aug 13:41:17.9 from 192.168.88.1
dns,packet question: www.facebook.com:A:IN in 13-Aug 13:41:17.10
from 192.168.88.1
dns,packet --- got answer from 8.8.8.8:53: in 13-Aug 13:41:17.10
from 192.168.88.1
dns,packet id:fef rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in 13-
Aug 13:41:17.10 from 192.168.88.1
dns,packet question: www.facebook.com:A:IN in 13-Aug 13:41:17.10
from 192.168.88.1
dns,packet answer: in 13-Aug 13:41:17.10 from 192.168.88.1
dns,packet <www.facebook.com:CNAME:3540=star-
mini.c10r.facebook.com> in 13-Aug 13:41:17.10 from 192.168.88.1
dns,packet <star-mini.c10r.facebook.com:A:51=31.13.78.35> in 13-
Aug 13:41:17.10 from 192.168.88.1
dns,packet authority: in 13-Aug 13:41:17.10 from 192.168.88.1
dns,packet <c10r.facebook.com:NS:3599=a.ns.c10r.facebook.com> in
13-Aug 13:41:17.11 from 192.168.88.1
dns,packet <c10r.facebook.com:NS:3599=b.ns.c10r.facebook.com> in
13-Aug 13:41:17.11 from 192.168.88.1
dns,packet additional: in 13-Aug 13:41:17.11 from 192.168.88.1
dns,packet
<a.ns.c10r.facebook.com:AAAA:3599=2a03:2880:fffe:b:face:b00c:0:99>
in 13-Aug 13:41:17.11 from 192.168.88.1
dns,packet <a.ns.c10r.facebook.com:A:3599=69.171.239.11> in 13-Aug
13:41:17.11 from 192.168.88.1
dns,packet
<b.ns.c10r.facebook.com:AAAA:3599=2a03:2880:ffff:b:face:b00c:0:99>
in 13-Aug 13:41:17.11 from 192.168.88.1
dns,packet <b.ns.c10r.facebook.com:A:3599=69.171.255.11> in 13-Aug
13:41:17.11 from 192.168.88.1
dns done query: #3925 www.facebook.com 31.13.78.35 in 13-Aug
13:41:17.12 from 192.168.88.1
dns,packet --- sending reply to 192.168.88.11:49344: in 13-Aug
13:41:17.12 from 192.168.88.1
dns,packet id:36d9 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 13:41:17.12 from 192.168.88.1
dns,packet question: www.facebook.com:A:IN in 13-Aug 13:41:17.12
from 192.168.88.1
dns,packet answer: in 13-Aug 13:41:17.12 from 192.168.88.1
dns,packet <www.facebook.com:CNAME:3540=star-
mini.c10r.facebook.com> in 13-Aug 13:41:17.12 from 192.168.88.1
dns,packet <star-mini.c10r.facebook.com:A:51=31.13.78.35> in 13-
Aug 13:41:17.12 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:36865->8.8.8.8:53, len 62 in 13-Aug 13:41:17.19 from
192.168.88.1
dns,packet --- got query from 192.168.66.20:64399: in 13-Aug
13:41:19.62 from 192.168.88.1
dns,packet id:8b52 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
```

```
13-Aug 13:41:19.62 from 192.168.88.1
dns,packet question: fonts.gstatic.com:A:IN in 13-Aug 13:41:19.62
from 192.168.88.1
dns query from 192.168.66.20: #3926 fonts.gstatic.com. A in 13-Aug
13:41:19.62 from 192.168.88.1
dns,packet --- sending udp query to 8.8.8.8:53: in 13-Aug
13:41:19.62 from 192.168.88.1
dns,packet id:93d rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in 13-
Aug 13:41:19.62 from 192.168.88.1
dns,packet question: fonts.gstatic.com:A:IN in 13-Aug 13:41:19.62
from 192.168.88.1
dns,packet --- got answer from 8.8.8.8:53: in 13-Aug 13:41:19.62
from 192.168.88.1
dns,packet id:93d rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in 13-
Aug 13:41:19.62 from 192.168.88.1
dns,packet question: fonts.gstatic.com:A:IN in 13-Aug 13:41:19.63
from 192.168.88.1
dns,packet answer: in 13-Aug 13:41:19.63 from 192.168.88.1
dns,packet <fonts.gstatic.com:CNAME:72=gstaticadssl.l.google.com>
in 13-Aug 13:41:19.63 from 192.168.88.1
dns,packet <gstaticadssl.l.google.com:A:2=74.125.68.94> in 13-Aug
13:41:19.63 from 192.168.88.1
dns done query: #3926 fonts.gstatic.com 74.125.68.94 in 13-Aug
13:41:19.63 from 192.168.88.1
dns,packet --- sending reply to 192.168.66.20:64399: in 13-Aug
13:41:19.63 from 192.168.88.1
dns,packet id:8b52 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 13:41:19.63 from 192.168.88.1
dns,packet question: fonts.gstatic.com:A:IN in 13-Aug 13:41:19.63
from 192.168.88.1
dns,packet answer: in 13-Aug 13:41:19.63 from 192.168.88.1
dns,packet <fonts.gstatic.com:CNAME:72=gstaticadssl.l.google.com>
in 13-Aug 13:41:19.63 from 192.168.88.1
dns,packet <gstaticadssl.l.google.com:A:2=74.125.68.94> in 13-Aug
13:41:19.63 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:47322->8.8.8.8:53, len 63 in 13-Aug 13:41:19.71 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:59911-
>74.125.68.94:80, len 52 in 13-Aug 13:41:19.71 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:59912-
>203.114.72.72:80, len 52 in 13-Aug 13:41:19.71 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:59913-
>203.114.72.72:80, len 52 in 13-Aug 13:41:20.8 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto UDP, 192.168.66.20:64401-
>172.217.26.78:443, len 1378 in 13-Aug 13:41:23.93 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:59914-
>172.217.26.78:443, len 52 in 13-Aug 13:41:24.45 from 192.168.88.1
dns,packet --- got query from 192.168.66.20:56517: in 13-Aug
13:41:31.16 from 192.168.88.1
```

```
dns,packet id:767 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in 13-
Aug 13:41:31.16 from 192.168.88.1
dns,packet question: facebook.com:A:IN in 13-Aug 13:41:31.16 from
192.168.88.1
dns query from 192.168.66.20: #3927 facebook.com. A in 13-Aug
13:41:31.16 from 192.168.88.1
dns,packet --- sending udp query to 8.8.8.8:53: in 13-Aug
13:41:31.16 from 192.168.88.1
dns,packet id:48b5 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 13:41:31.16 from 192.168.88.1
dns,packet question: facebook.com:A:IN in 13-Aug 13:41:31.17 from
192.168.88.1
dns,packet --- got answer from 8.8.8.8:53: in 13-Aug 13:41:31.17
from 192.168.88.1
dns,packet id:48b5 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 13:41:31.17 from 192.168.88.1
dns,packet question: facebook.com:A:IN in 13-Aug 13:41:31.17 from
192.168.88.1
dns,packet answer: in 13-Aug 13:41:31.17 from 192.168.88.1
dns,packet <facebook.com:A:283=69.171.230.68> in 13-Aug
13:41:31.17 from 192.168.88.1
dns done query: #3927 facebook.com 69.171.230.68 in 13-Aug
13:41:31.17 from 192.168.88.1
dns,packet --- sending reply to 192.168.66.20:56517: in 13-Aug
13:41:31.17 from 192.168.88.1
dns,packet id:767 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in 13-
Aug 13:41:31.18 from 192.168.88.1
dns,packet question: facebook.com:A:IN in 13-Aug 13:41:31.18 from
192.168.88.1
dns,packet answer: in 13-Aug 13:41:31.18 from 192.168.88.1
dns,packet <facebook.com:A:283=69.171.230.68> in 13-Aug
13:41:31.18 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:49159->8.8.8.8:53, len 58 in 13-Aug 13:41:31.25 from
192.168.88.1
dns,packet --- got query from 192.168.66.20:50577: in 13-Aug
13:41:31.49 from 192.168.88.1
dns,packet id:f2f8 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 13:41:31.50 from 192.168.88.1
dns,packet question: muffingroup.com:A:IN in 13-Aug 13:41:31.50
from 192.168.88.1
dns query from 192.168.66.20: #3928 muffingroup.com. A in 13-Aug
13:41:31.50 from 192.168.88.1
dns,packet --- sending udp query to 8.8.8.8:53: in 13-Aug
13:41:31.50 from 192.168.88.1
dns,packet id:792a rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 13:41:31.50 from 192.168.88.1
dns,packet question: muffingroup.com:A:IN in 13-Aug 13:41:31.50
from 192.168.88.1
dns,packet --- got query from 192.168.66.20:62686: in 13-Aug
13:41:31.50 from 192.168.88.1
dns,packet id:faaf rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 13:41:31.50 from 192.168.88.1
dns,packet question: pin.bbm.com:A:IN in 13-Aug 13:41:31.50 from
192.168.88.1
dns query from 192.168.66.20: #3929 pin.bbm.com. A in 13-Aug
```

```
13:41:31.51 from 192.168.88.1
dns,packet --- sending udp query to 8.8.8.8:53: in 13-Aug
13:41:31.51 from 192.168.88.1
dns,packet id:3596 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 13:41:31.51 from 192.168.88.1
dns,packet question: pin.bbm.com:A:IN in 13-Aug 13:41:31.51 from
192.168.88.1
dns,packet --- got answer from 8.8.8.8:53: in 13-Aug 13:41:31.51
from 192.168.88.1
dns,packet id:3596 rd:1 tc:0 aa:0 qr:1 ra:0 QUERY 'no error' in
13-Aug 13:41:31.51 from 192.168.88.1
dns,packet question: pin.bbm.com:A:IN in 13-Aug 13:41:31.51 from
192.168.88.1
dns,packet answer: in 13-Aug 13:41:31.51 from 192.168.88.1
dns,packet <pin.bbm.com:A:473=208.65.77.151> in 13-Aug 13:41:31.51
from 192.168.88.1
dns done query: #3929 pin.bbm.com 208.65.77.151 in 13-Aug
13:41:31.51 from 192.168.88.1
dns,packet --- sending reply to 192.168.66.20:62686: in 13-Aug
13:41:31.51 from 192.168.88.1
dns,packet id:faaf rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 13:41:31.51 from 192.168.88.1
dns,packet question: pin.bbm.com:A:IN in 13-Aug 13:41:31.51 from
192.168.88.1
dns,packet answer: in 13-Aug 13:41:31.52 from 192.168.88.1
dns,packet <pin.bbm.com:A:473=208.65.77.151> in 13-Aug 13:41:31.52
from 192.168.88.1
dns,packet --- got answer from 8.8.8.8:53: in 13-Aug 13:41:31.54
from 192.168.88.1
dns,packet id:792a rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 13:41:31.54 from 192.168.88.1
dns,packet question: muffingroup.com:A:IN in 13-Aug 13:41:31.54
from 192.168.88.1
dns,packet answer: in 13-Aug 13:41:31.54 from 192.168.88.1
dns,packet <muffingroup.com:A:300=164.132.159.119> in 13-Aug
13:41:31.54 from 192.168.88.1
dns,packet additional: in 13-Aug 13:41:31.54 from 192.168.88.1
dns,packet <:UNKNOWN (41):32768=rawbytes:0> in 13-Aug 13:41:31.54
from 192.168.88.1
dns done query: #3928 muffingroup.com 164.132.159.119 in 13-Aug
13:41:31.55 from 192.168.88.1
dns,packet --- sending reply to 192.168.66.20:50577: in 13-Aug
13:41:31.55 from 192.168.88.1
dns,packet id:f2f8 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 13:41:31.55 from 192.168.88.1
dns,packet question: muffingroup.com:A:IN in 13-Aug 13:41:31.55
from 192.168.88.1
dns,packet answer: in 13-Aug 13:41:31.55 from 192.168.88.1
dns,packet <muffingroup.com:A:300=164.132.159.119> in 13-Aug
13:41:31.55 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:53591->8.8.8.8:53, len 61 in 13-Aug 13:41:31.59 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:53709->8.8.8.8:53, len 57 in 13-Aug 13:41:31.59 from
192.168.88.1
```

```
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:59915-
>52.196.33.60:443, len 52 in 13-Aug 13:41:32.3 from 192.168.88.1
dns,packet --- got query from 192.168.66.20:49895: in 13-Aug
13:41:34.8 from 192.168.88.1
dns,packet id:4244 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 13:41:34.8 from 192.168.88.1
dns,packet question: a.tribalfusion.com:A:IN in 13-Aug 13:41:34.8
from 192.168.88.1
dns query from 192.168.66.20: #3930 a.tribalfusion.com. A in 13-
Aug 13:41:34.8 from 192.168.88.1
dns,packet --- sending udp query to 8.8.4.4:53: in 13-Aug
13:41:34.8 from 192.168.88.1
dns,packet id:45f1 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 13:41:34.9 from 192.168.88.1
dns,packet question: a.tribalfusion.com:A:IN in 13-Aug 13:41:34.9
from 192.168.88.1
dns,packet --- got query from 192.168.66.20:52438: in 13-Aug
13:41:34.9 from 192.168.88.1
dns,packet id:ed64 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 13:41:34.9 from 192.168.88.1
dns,packet question: m.addthisedge.com:A:IN in 13-Aug 13:41:34.9
from 192.168.88.1
dns query from 192.168.66.20: #3931 m.addthisedge.com. A in 13-Aug
13:41:34.9 from 192.168.88.1
dns done query: #3931 dns name exists, but no appropriate record
in 13-Aug 13:41:34.9 from 192.168.88.1
dns,packet --- sending reply to 192.168.66.20:52438: in 13-Aug
13:41:34.9 from 192.168.88.1
dns,packet id:ed64 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 13:41:34.9 from 192.168.88.1
dns,packet question: m.addthisedge.com:A:IN in 13-Aug 13:41:34.9
from 192.168.88.1
dns,packet answer: in 13-Aug 13:41:34.9 from 192.168.88.1
dns,packet
<m.addthisedge.com:CNAME:6=m.addthisedge.com.cdn.cloudflare.net>
in 13-Aug 13:41:34.9 from 192.168.88.1
dns,packet
<m.addthisedge.com.cdn.cloudflare.net:A:147=104.16.25.235> in 13-
Aug 13:41:34.10 from 192.168.88.1
dns,packet
<m.addthisedge.com.cdn.cloudflare.net:A:147=104.16.23.235> in 13-
Aug 13:41:34.10 from 192.168.88.1
dns,packet
<m.addthisedge.com.cdn.cloudflare.net:A:147=104.16.27.235> in 13-
Aug 13:41:34.10 from 192.168.88.1
dns,packet
<m.addthisedge.com.cdn.cloudflare.net:A:147=104.16.26.235> in 13-
Aug 13:41:34.10 from 192.168.88.1
dns,packet
<m.addthisedge.com.cdn.cloudflare.net:A:147=104.16.24.235> in 13-
Aug 13:41:34.10 from 192.168.88.1
dns,packet --- got answer from 8.8.4.4:53: in 13-Aug 13:41:34.10
from 192.168.88.1
dns,packet id:45f1 rd:1 tc:0 aa:0 qr:1 ra:0 QUERY 'no error' in
13-Aug 13:41:34.10 from 192.168.88.1
```

```
dns,packet question: a.tribalfusion.com:A:IN in 13-Aug 13:41:34.10
from 192.168.88.1
dns,packet answer: in 13-Aug 13:41:34.10 from 192.168.88.1
dns,packet <a.tribalfusion.com:A:3600=204.11.109.68> in 13-Aug
13:41:34.10 from 192.168.88.1
dns,packet <a.tribalfusion.com:A:3600=204.11.109.67> in 13-Aug
13:41:34.10 from 192.168.88.1
dns,packet <a.tribalfusion.com:A:3600=204.11.109.65> in 13-Aug
13:41:34.10 from 192.168.88.1
dns,packet <a.tribalfusion.com:A:3600=204.11.109.66> in 13-Aug
13:41:34.11 from 192.168.88.1
dns done query: #3930 a.tribalfusion.com 204.11.109.68 in 13-Aug
13:41:34.11 from 192.168.88.1
dns,packet --- sending reply to 192.168.66.20:49895: in 13-Aug
13:41:34.11 from 192.168.88.1
dns,packet id:4244 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 13:41:34.11 from 192.168.88.1
dns,packet question: a.tribalfusion.com:A:IN in 13-Aug 13:41:34.11
from 192.168.88.1
dns,packet answer: in 13-Aug 13:41:34.11 from 192.168.88.1
dns,packet <a.tribalfusion.com:A:3600=204.11.109.68> in 13-Aug
13:41:34.11 from 192.168.88.1
dns,packet <a.tribalfusion.com:A:3600=204.11.109.67> in 13-Aug
13:41:34.11 from 192.168.88.1
dns,packet <a.tribalfusion.com:A:3600=204.11.109.65> in 13-Aug
13:41:34.11 from 192.168.88.1
dns,packet <a.tribalfusion.com:A:3600=204.11.109.66> in 13-Aug
13:41:34.11 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:60953->8.8.4.4:53, len 64 in 13-Aug 13:41:34.17 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:59916-
>50.97.236.98:80, len 52 in 13-Aug 13:41:34.17 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:59917-
>50.97.236.98:80, len 52 in 13-Aug 13:41:34.17 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:59918-
>104.16.25.235:80, len 52 in 13-Aug 13:41:34.17 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:59919-
>104.16.25.235:80, len 52 in 13-Aug 13:41:34.17 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:59920-
>104.16.25.235:80, len 52 in 13-Aug 13:41:34.17 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:59921-
>204.11.109.68:80, len 52 in 13-Aug 13:41:34.17 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:59922-
>204.11.109.68:80, len 52 in 13-Aug 13:41:34.18 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:59923-
>204.11.109.68:80, len 52 in 13-Aug 13:41:34.18 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
```

```
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:59924-
>104.16.18.35:80, len 52 in 13-Aug 13:41:34.36 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:59925-
>192.229.237.25:80, len 52 in 13-Aug 13:41:34.68 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:59926-
>192.229.237.25:80, len 52 in 13-Aug 13:41:34.68 from 192.168.88.1
dns,packet --- got query from 192.168.66.20:61095: in 13-Aug
13:41:35.30 from 192.168.88.1
dns,packet id:2c9e rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 13:41:35.30 from 192.168.88.1
dns,packet question: staticxx.facebook.com:A:IN in 13-Aug
13:41:35.31 from 192.168.88.1
dns query from 192.168.66.20: #3932 staticxx.facebook.com. A in
13-Aug 13:41:35.31 from 192.168.88.1
dns,packet --- sending udp query to 192.168.0.1:53: in 13-Aug
13:41:35.31 from 192.168.88.1
dns,packet id:4591 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 13:41:35.31 from 192.168.88.1
dns,packet question: staticxx.facebook.com:A:IN in 13-Aug
13:41:35.31 from 192.168.88.1
dns,packet --- got answer from 192.168.0.1:53: in 13-Aug
13:41:35.31 from 192.168.88.1
dns,packet id:4591 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 13:41:35.31 from 192.168.88.1
dns,packet question: staticxx.facebook.com:A:IN in 13-Aug
13:41:35.32 from 192.168.88.1
dns,packet answer: in 13-Aug 13:41:35.32 from 192.168.88.1
dns,packet
<staticxx.facebook.com:CNAME:1921=scontent.xx.fbcdn.net> in 13-Aug
13:41:35.32 from 192.168.88.1
dns,packet <scontent.xx.fbcdn.net:A:47=31.13.78.17> in 13-Aug
13:41:35.34 from 192.168.88.1
dns,packet authority: in 13-Aug 13:41:35.34 from 192.168.88.1
dns,packet <xx.fbcdn.net:NS:3600=a.ns.xx.fbcdn.net> in 13-Aug
13:41:35.34 from 192.168.88.1
dns,packet <xx.fbcdn.net:NS:3600=b.ns.xx.fbcdn.net> in 13-Aug
13:41:35.34 from 192.168.88.1
dns,packet additional: in 13-Aug 13:41:35.34 from 192.168.88.1
dns,packet
<a.ns.xx.fbcdn.net:AAAA:3600=2a03:2880:fffe:b:face:b00c:0:99> in
13-Aug 13:41:35.34 from 192.168.88.1
dns,packet <a.ns.xx.fbcdn.net:A:3600=69.171.239.11> in 13-Aug
13:41:35.34 from 192.168.88.1
dns,packet
<b.ns.xx.fbcdn.net:AAAA:3600=2a03:2880:ffff:b:face:b00c:0:99> in
13-Aug 13:41:35.34 from 192.168.88.1
dns,packet <b.ns.xx.fbcdn.net:A:3600=69.171.255.11> in 13-Aug
13:41:35.34 from 192.168.88.1
dns done query: #3932 staticxx.facebook.com 31.13.78.17 in 13-Aug
13:41:35.34 from 192.168.88.1
dns,packet --- sending reply to 192.168.66.20:61095: in 13-Aug
13:41:35.35 from 192.168.88.1
dns,packet id:2c9e rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 13:41:35.35 from 192.168.88.1
```

```
dns,packet question: staticxx.facebook.com:A:IN in 13-Aug
13:41:35.35 from 192.168.88.1
dns,packet answer: in 13-Aug 13:41:35.35 from 192.168.88.1
dns,packet
<staticxx.facebook.com:CNAME:1921=scontent.xx.fbcdn.net> in 13-Aug
13:41:35.35 from 192.168.88.1
dns,packet <scontent.xx.fbcdn.net:A:47=31.13.78.17> in 13-Aug
13:41:35.35 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:32796->192.168.0.1:53, len 67 in 13-Aug 13:41:35.40
from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:59927-
>31.13.78.17:443, len 52 in 13-Aug 13:41:35.40 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:59928-
>31.13.78.17:443, len 52 in 13-Aug 13:41:36.64 from 192.168.88.1
dns,packet --- got query from 192.168.88.11:65514: in 13-Aug
13:41:38.63 from 192.168.88.1
dns,packet id:42f3 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 13:41:38.63 from 192.168.88.1
dns,packet question: 1-edge-chat.facebook.com:A:IN in 13-Aug
13:41:38.63 from 192.168.88.1
dns query from 192.168.88.11: #3933 1-edge-chat.facebook.com. A in
13-Aug 13:41:38.63 from 192.168.88.1
dns,packet --- sending udp query to 192.168.0.1:53: in 13-Aug
13:41:38.63 from 192.168.88.1
dns,packet id:5c74 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 13:41:38.63 from 192.168.88.1
dns,packet question: 1-edge-chat.facebook.com:A:IN in 13-Aug
13:41:38.64 from 192.168.88.1
dns,packet --- got answer from 192.168.0.1:53: in 13-Aug
13:41:38.64 from 192.168.88.1
dns,packet id:5c74 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 13:41:38.64 from 192.168.88.1
dns,packet question: 1-edge-chat.facebook.com:A:IN in 13-Aug
13:41:38.64 from 192.168.88.1
dns,packet answer: in 13-Aug 13:41:38.64 from 192.168.88.1
dns,packet <1-edge-
chat.facebook.com:CNAME:247=star.c10r.facebook.com> in 13-Aug
13:41:38.64 from 192.168.88.1
dns,packet <star.c10r.facebook.com:A:50=31.13.78.13> in 13-Aug
13:41:38.64 from 192.168.88.1
dns done query: #3933 1-edge-chat.facebook.com 31.13.78.13 in 13-
Aug 13:41:38.64 from 192.168.88.1
dns,packet --- sending reply to 192.168.88.11:65514: in 13-Aug
13:41:38.64 from 192.168.88.1
dns,packet id:42f3 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 13:41:38.64 from 192.168.88.1
dns,packet question: 1-edge-chat.facebook.com:A:IN in 13-Aug
13:41:38.64 from 192.168.88.1
dns,packet answer: in 13-Aug 13:41:38.64 from 192.168.88.1
dns,packet <1-edge-
chat.facebook.com:CNAME:1242=star.c10r.facebook.com> in 13-Aug
13:41:38.64 from 192.168.88.1
dns,packet <star.c10r.facebook.com:A:50=31.13.78.13> in 13-Aug
```

```
13:41:38.65 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:59869->192.168.0.1:53, len 70 in 13-Aug 13:41:38.73
from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
9c:8e:99:41:73:c4, proto TCP (SYN), 192.168.88.11:60498-
>192.168.0.1:49152, len 52 in 13-Aug 13:41:40.98 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto UDP, 192.168.66.20:61099-
>74.125.130.113:443, len 1378 in 13-Aug 13:41:52.83 from
192.168.88.1
dns,packet --- got query from 192.168.66.20:53435: in 13-Aug
13:42:21.97 from 192.168.88.1
dns,packet id:25b5 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 13:42:21.97 from 192.168.88.1
dns,packet question: clients4.google.com:A:IN in 13-Aug
13:42:21.97 from 192.168.88.1
dns query from 192.168.66.20: #3934 clients4.google.com. A in 13-
Aug 13:42:21.97 from 192.168.88.1
dns,packet --- sending udp query to 192.168.0.1:53: in 13-Aug
13:42:21.97 from 192.168.88.1
dns,packet id:d2b6 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 13:42:21.97 from 192.168.88.1
dns,packet question: clients4.google.com:A:IN in 13-Aug
13:42:21.97 from 192.168.88.1
dns,packet --- got answer from 192.168.0.1:53: in 13-Aug
13:42:21.98 from 192.168.88.1
dns,packet id:d2b6 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 13:42:21.98 from 192.168.88.1
dns,packet question: clients4.google.com:A:IN in 13-Aug
13:42:21.98 from 192.168.88.1
dns,packet answer: in 13-Aug 13:42:21.98 from 192.168.88.1
dns,packet <clients4.google.com:CNAME:248=clients.l.google.com> in
13-Aug 13:42:21.98 from 192.168.88.1
dns,packet <clients.l.google.com:A:57=74.125.200.100> in 13-Aug
13:42:21.98 from 192.168.88.1
dns,packet <clients.l.google.com:A:57=74.125.200.113> in 13-Aug
13:42:21.98 from 192.168.88.1
dns,packet <clients.l.google.com:A:57=74.125.200.139> in 13-Aug
13:42:21.98 from 192.168.88.1
dns,packet <clients.l.google.com:A:57=74.125.200.101> in 13-Aug
13:42:21.98 from 192.168.88.1
dns,packet <clients.l.google.com:A:57=74.125.200.102> in 13-Aug
13:42:21.99 from 192.168.88.1
dns,packet <clients.l.google.com:A:57=74.125.200.138> in 13-Aug
13:42:21.99 from 192.168.88.1
dns done query: #3934 clients4.google.com 74.125.200.100 in 13-Aug
13:42:21.99 from 192.168.88.1
dns,packet --- sending reply to 192.168.66.20:53435: in 13-Aug
13:42:21.99 from 192.168.88.1
dns,packet id:25b5 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 13:42:21.99 from 192.168.88.1
dns,packet question: clients4.google.com:A:IN in 13-Aug
13:42:21.99 from 192.168.88.1
dns,packet answer: in 13-Aug 13:42:21.99 from 192.168.88.1
dns,packet <clients4.google.com:CNAME:248=clients.l.google.com> in
```

```
13-Aug 13:42:21.99 from 192.168.88.1
dns,packet <clients.l.google.com:A:57=74.125.200.100> in 13-Aug
13:42:21.99 from 192.168.88.1
dns,packet <clients.l.google.com:A:57=74.125.200.138> in 13-Aug
13:42:22.0 from 192.168.88.1
dns,packet <clients.l.google.com:A:57=74.125.200.113> in 13-Aug
13:42:22.0 from 192.168.88.1
dns,packet <clients.l.google.com:A:57=74.125.200.139> in 13-Aug
13:42:22.0 from 192.168.88.1
dns,packet <clients.l.google.com:A:57=74.125.200.101> in 13-Aug
13:42:22.0 from 192.168.88.1
dns,packet <clients.l.google.com:A:57=74.125.200.102> in 13-Aug
13:42:22.0 from 192.168.88.1

dns,packet <ocsp-
ds.ws.symantec.com.edgekey.net:CNAME:19=e8218.dscb1.akamaiedge.net
> in 13-Aug 14:52:17.51 from 192.168.88.1
dns,packet <e8218.dscb1.akamaiedge.net:A:15=23.15.155.27> in 13-
Aug 14:52:18.30 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:59926->8.8.8.8:53, len 58 in 13-Aug 14:52:18.30 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:60246-
>23.15.155.27:80, len 52 in 13-Aug 14:52:18.30 from 192.168.88.1
dhcp,debug,packet dhcp1 received inform with id 3603798449 from
192.168.88.11 in 13-Aug 14:52:18.30 from 192.168.88.1
dhcp,debug,packet     ciaddr = 192.168.88.11 in 13-Aug 14:52:18.30
from 192.168.88.1
dhcp,debug,packet     chaddr = 9C:8E:99:41:73:C4 in 13-Aug
14:52:18.30 from 192.168.88.1
dhcp,debug,packet     Msg-Type = inform in 13-Aug 14:52:18.30 from
192.168.88.1
dhcp,debug,packet     Client-Id = 01-9C-8E-99-41-73-C4 in 13-Aug
14:52:18.30 from 192.168.88.1
dhcp,debug,packet     Host-Name = "Vanasea" in 13-Aug 14:52:18.30
from 192.168.88.1
dhcp,debug,packet     Class-Id = "MSFT 5.0" in 13-Aug 14:52:18.31
from 192.168.88.1
dhcp,debug,packet     Parameter-List = Subnet-Mask,Domain-
Name,Router,Domain-Server,NETBIOS-Name-Server,NETBIOS-Node-
Type,NETBIOS-Scope,Router-Discovery,Static-Route,Classless-
Route,MS-Classless-Route,Vendor-Specific,Auto-Proxy-Config in 13-
Aug 14:52:18.31 from 192.168.88.1
dhcp,debug,packet dhcp1 sending ack with id 3603798449 to
192.168.88.11 in 13-Aug 14:52:18.31 from 192.168.88.1
dhcp,debug,packet     ciaddr = 192.168.88.11 in 13-Aug 14:52:18.31
from 192.168.88.1
dhcp,debug,packet     siaddr = 192.168.88.1 in 13-Aug 14:52:18.31
from 192.168.88.1
dhcp,debug,packet     chaddr = 9C:8E:99:41:73:C4 in 13-Aug
14:52:18.31 from 192.168.88.1
dhcp,debug,packet     Msg-Type = ack in 13-Aug 14:52:18.31 from
192.168.88.1
dhcp,debug,packet     Server-Id = 192.168.88.1 in 13-Aug
14:52:18.31 from 192.168.88.1
```

```
dhcp,debug,packet     Subnet-Mask = 255.255.255.0 in 13-Aug
14:52:18.31 from 192.168.88.1
dhcp,debug,packet     Router = 192.168.88.1 in 13-Aug 14:52:18.31
from 192.168.88.1
dhcp,debug,packet     Domain-Server = 192.168.88.1,192.168.0.1 in
13-Aug 14:52:18.31 from 192.168.88.1
dns,packet --- got query from 192.168.88.11:57253: in 13-Aug
14:52:18.31 from 192.168.88.1
dns,packet id:b07f rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 14:52:18.31 from 192.168.88.1
dns,packet question: settings-win.data.microsoft.com:A:IN in 13-
Aug 14:52:18.32 from 192.168.88.1
dns query from 192.168.88.11: #4370 settings-
win.data.microsoft.com. A in 13-Aug 14:52:18.32 from 192.168.88.1
dns,packet --- sending udp query to 8.8.8.8:53: in 13-Aug
14:52:18.32 from 192.168.88.1
dns,packet id:6a0f rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 14:52:18.32 from 192.168.88.1
dns,packet question: settings-win.data.microsoft.com:A:IN in 13-
Aug 14:52:18.32 from 192.168.88.1
dns,packet --- got answer from 8.8.8.8:53: in 13-Aug 14:52:18.32
from 192.168.88.1
dns,packet id:6a0f rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 14:52:18.32 from 192.168.88.1
dns,packet question: settings-win.data.microsoft.com:A:IN in 13-
Aug 14:52:18.32 from 192.168.88.1
dns,packet answer: in 13-Aug 14:52:18.32 from 192.168.88.1
dns,packet <settings-win.data.microsoft.com:CNAME:3145=asimov-
win.settings.data.microsoft.com.akadns.net> in 13-Aug 14:52:18.32
from 192.168.88.1
dns,packet <asimov-
win.settings.data.microsoft.com.akadns.net:CNAME:257=geo.settings.
data.microsoft.com.akadns.net> in 13-Aug 14:52:18.32 from
192.168.88.1
dns,packet
<geo.settings.data.microsoft.com.akadns.net:CNAME:243=hk2.settings
.data.microsoft.com.akadns.net> in 13-Aug 14:52:18.32 from
192.168.88.1
dns,packet
<hk2.settings.data.microsoft.com.akadns.net:A:172=111.221.29.253>
in 13-Aug 14:52:18.32 from 192.168.88.1
dns done query: #4370 settings-win.data.microsoft.com
111.221.29.253 in 13-Aug 14:52:18.32 from 192.168.88.1
dns,packet --- sending reply to 192.168.88.11:57253: in 13-Aug
14:52:18.32 from 192.168.88.1
dns,packet id:b07f rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 14:52:18.32 from 192.168.88.1
dns,packet question: settings-win.data.microsoft.com:A:IN in 13-
Aug 14:52:18.32 from 192.168.88.1
dns,packet answer: in 13-Aug 14:52:18.32 from 192.168.88.1
dns,packet <settings-win.data.microsoft.com:CNAME:3145=asimov-
win.settings.data.microsoft.com.akadns.net> in 13-Aug 14:52:18.33
from 192.168.88.1
dns,packet <asimov-
win.settings.data.microsoft.com.akadns.net:CNAME:257=geo.settings.
data.microsoft.com.akadns.net> in 13-Aug 14:52:18.33 from
```

```
192.168.88.1
dns,packet
<geo.settings.data.microsoft.com.akadns.net:CNAME:243=hk2.settings
.data.microsoft.com.akadns.net> in 13-Aug 14:52:18.33 from
192.168.88.1
dns,packet
<hk2.settings.data.microsoft.com.akadns.net:A:172=111.221.29.253>
in 13-Aug 14:52:18.33 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:49343->8.8.8.8:53, len 77 in 13-Aug 14:52:18.33 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
9c:8e:99:41:73:c4, proto TCP (SYN), 192.168.88.11:60693-
>111.221.29.253:443, len 52 in 13-Aug 14:52:18.33 from
192.168.88.1
dns,packet --- got query from 192.168.66.20:50835: in 13-Aug
14:52:19.48 from 192.168.88.1
dns,packet id:5547 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 14:52:19.49 from 192.168.88.1
dns,packet question: service.weather.microsoft.com:A:IN in 13-Aug
14:52:19.49 from 192.168.88.1
dns query from 192.168.66.20: #4371 service.weather.microsoft.com.
A in 13-Aug 14:52:19.49 from 192.168.88.1
dns,packet --- sending udp query to 8.8.8.8:53: in 13-Aug
14:52:19.49 from 192.168.88.1
dns,packet id:97f rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in 13-
Aug 14:52:19.49 from 192.168.88.1
dns,packet question: service.weather.microsoft.com:A:IN in 13-Aug
14:52:19.49 from 192.168.88.1
dns,packet --- got answer from 8.8.8.8:53: in 13-Aug 14:52:19.49
from 192.168.88.1
dns,packet id:97f rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in 13-
Aug 14:52:19.49 from 192.168.88.1
dns,packet question: service.weather.microsoft.com:A:IN in 13-Aug
14:52:19.49 from 192.168.88.1
dns,packet answer: in 13-Aug 14:52:19.49 from 192.168.88.1
dns,packet
<service.weather.microsoft.com:CNAME:3334=wildcard.weather.microso
ft.com.edgekey.net> in 13-Aug 14:52:19.49 from 192.168.88.1
dns,packet
<wildcard.weather.microsoft.com.edgekey.net:CNAME:817=e7070.g.akam
aiedge.net> in 13-Aug 14:52:19.49 from 192.168.88.1
dns,packet <e7070.g.akamaiedge.net:A:16=104.93.213.33> in 13-Aug
14:52:19.49 from 192.168.88.1
dns done query: #4371 service.weather.microsoft.com 104.93.213.33
in 13-Aug 14:52:19.49 from 192.168.88.1
dns,packet --- sending reply to 192.168.66.20:50835: in 13-Aug
14:52:19.49 from 192.168.88.1
dns,packet id:5547 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 14:52:19.50 from 192.168.88.1
dns,packet question: service.weather.microsoft.com:A:IN in 13-Aug
14:52:19.50 from 192.168.88.1
dns,packet answer: in 13-Aug 14:52:19.50 from 192.168.88.1
dns,packet
<service.weather.microsoft.com:CNAME:3334=wildcard.weather.microso
ft.com.edgekey.net> in 13-Aug 14:52:19.50 from 192.168.88.1
```

```
dns,packet
<wildcard.weather.microsoft.com.edgekey.net:CNAME:817=e7070.g.akam
aiedge.net> in 13-Aug 14:52:19.50 from 192.168.88.1
dns,packet <e7070.g.akamaiedge.net:A:16=104.93.213.33> in 13-Aug
14:52:19.50 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:56270->8.8.8.8:53, len 75 in 13-Aug 14:52:19.58 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:60247-
>104.93.213.33:80, len 52 in 13-Aug 14:52:19.59 from 192.168.88.1
dns,packet --- got query from 192.168.66.20:55154: in 13-Aug
14:52:19.59 from 192.168.88.1
dns,packet id:5886 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 14:52:19.59 from 192.168.88.1
dns,packet question: finance.services.appex.bing.com:A:IN in 13-
Aug 14:52:19.59 from 192.168.88.1
dns query from 192.168.66.20: #4372
finance.services.appex.bing.com. A in 13-Aug 14:52:19.59 from
192.168.88.1
dns,packet --- sending udp query to 8.8.8.8:53: in 13-Aug
14:52:19.67 from 192.168.88.1
dns,packet id:d1dc rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 14:52:19.67 from 192.168.88.1
dns,packet question: finance.services.appex.bing.com:A:IN in 13-
Aug 14:52:19.67 from 192.168.88.1
dns,packet --- got answer from 8.8.8.8:53: in 13-Aug 14:52:19.67
from 192.168.88.1
dns,packet id:d1dc rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 14:52:19.67 from 192.168.88.1
dns,packet question: finance.services.appex.bing.com:A:IN in 13-
Aug 14:52:19.67 from 192.168.88.1
dns,packet answer: in 13-Aug 14:52:19.67 from 192.168.88.1
dns,packet
<finance.services.appex.bing.com:CNAME:3352=finance.services.appex
.bing.com.edgekey.net> in 13-Aug 14:52:19.67 from 192.168.88.1
dns,packet
<finance.services.appex.bing.com.edgekey.net:CNAME:6933=e5212.g.ak
amaiedge.net> in 13-Aug 14:52:19.67 from 192.168.88.1
dns,packet <e5212.g.akamaiedge.net:A:11=104.93.232.82> in 13-Aug
14:52:19.68 from 192.168.88.1
dns done query: #4372 finance.services.appex.bing.com
104.93.232.82 in 13-Aug 14:52:19.68 from 192.168.88.1
dns,packet --- sending reply to 192.168.66.20:55154: in 13-Aug
14:52:19.68 from 192.168.88.1
dns,packet id:5886 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 14:52:19.68 from 192.168.88.1
dns,packet question: finance.services.appex.bing.com:A:IN in 13-
Aug 14:52:19.68 from 192.168.88.1
dns,packet answer: in 13-Aug 14:52:19.68 from 192.168.88.1
dns,packet
<finance.services.appex.bing.com:CNAME:3352=finance.services.appex
.bing.com.edgekey.net> in 13-Aug 14:52:19.68 from 192.168.88.1
dns,packet
<finance.services.appex.bing.com.edgekey.net:CNAME:6933=e5212.g.ak
amaiedge.net> in 13-Aug 14:52:19.68 from 192.168.88.1
```

```
dns,packet <e5212.g.akamaiedge.net:A:11=104.93.232.82> in 13-Aug
14:52:19.68 from 192.168.88.1
dns,packet --- got query from 192.168.66.20:58593: in 13-Aug
14:52:19.69 from 192.168.88.1
dns,packet id:4363 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 14:52:19.69 from 192.168.88.1
dns,packet question: clients4.google.com:A:IN in 13-Aug
14:52:19.69 from 192.168.88.1
dns query from 192.168.66.20: #4373 clients4.google.com. A in 13-
Aug 14:52:19.69 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:60248-
>118.98.93.17:80, len 52 in 13-Aug 14:52:19.69 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:60249-
>118.98.93.17:80, len 52 in 13-Aug 14:52:19.69 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:36942->8.8.8.8:53, len 77 in 13-Aug 14:52:19.69 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:60250-
>104.93.232.82:80, len 52 in 13-Aug 14:52:19.69 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:59592->8.8.8.8:53, len 65 in 13-Aug 14:52:19.69 from
192.168.88.1
dns,packet --- sending udp query to 8.8.8.8:53: in 13-Aug
14:52:19.69 from 192.168.88.1
dns,packet id:48ff rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 14:52:19.69 from 192.168.88.1
dns,packet question: clients4.google.com:A:IN in 13-Aug
14:52:19.69 from 192.168.88.1
dns,packet --- got answer from 8.8.8.8:53: in 13-Aug 14:52:19.69
from 192.168.88.1
dns,packet id:48ff rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 14:52:19.69 from 192.168.88.1
dns,packet question: clients4.google.com:A:IN in 13-Aug
14:52:19.69 from 192.168.88.1
dns,packet answer: in 13-Aug 14:52:19.69 from 192.168.88.1
dns,packet <clients4.google.com:CNAME:170=clients.l.google.com> in
13-Aug 14:52:19.69 from 192.168.88.1
dns,packet <clients.l.google.com:A:284=74.125.200.139> in 13-Aug
14:52:19.70 from 192.168.88.1
dns,packet <clients.l.google.com:A:284=74.125.200.101> in 13-Aug
14:52:19.70 from 192.168.88.1
dns,packet <clients.l.google.com:A:284=74.125.200.102> in 13-Aug
14:52:19.70 from 192.168.88.1
dns,packet <clients.l.google.com:A:284=74.125.200.113> in 13-Aug
14:52:19.70 from 192.168.88.1
dns,packet <clients.l.google.com:A:284=74.125.200.138> in 13-Aug
14:52:19.70 from 192.168.88.1
dns,packet <clients.l.google.com:A:284=74.125.200.100> in 13-Aug
14:52:19.70 from 192.168.88.1
dns done query: #4373 clients4.google.com 74.125.200.139 in 13-Aug
14:52:19.70 from 192.168.88.1
dns,packet --- sending reply to 192.168.66.20:58593: in 13-Aug
14:52:19.70 from 192.168.88.1
```

```
dns,packet id:4363 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 14:52:19.70 from 192.168.88.1
dns,packet question: clients4.google.com:A:IN in 13-Aug
14:52:19.70 from 192.168.88.1
dns,packet answer: in 13-Aug 14:52:19.70 from 192.168.88.1
dns,packet <clients4.google.com:CNAME:170=clients.l.google.com> in
13-Aug 14:52:19.70 from 192.168.88.1
dns,packet <clients.l.google.com:A:284=74.125.200.139> in 13-Aug
14:52:19.70 from 192.168.88.1
dns,packet <clients.l.google.com:A:284=74.125.200.101> in 13-Aug
14:52:19.70 from 192.168.88.1
dns,packet <clients.l.google.com:A:284=74.125.200.102> in 13-Aug
14:52:19.71 from 192.168.88.1
dns,packet <clients.l.google.com:A:284=74.125.200.113> in 13-Aug
14:52:19.71 from 192.168.88.1
dns,packet <clients.l.google.com:A:284=74.125.200.138> in 13-Aug
14:52:19.71 from 192.168.88.1
dns,packet <clients.l.google.com:A:284=74.125.200.100> in 13-Aug
14:52:19.71 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto UDP, 192.168.66.20:58594-
>74.125.200.139:443, len 1378 in 13-Aug 14:52:19.79 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:60251-
>74.125.200.139:443, len 52 in 13-Aug 14:52:19.91 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (ACK,PSH), 192.168.66.20:59787-
>111.221.29.171:443, len 157 in 13-Aug 14:52:20.79 from
192.168.88.1
dns,packet --- got query from 192.168.88.11:49152: in 13-Aug
14:52:21.32 from 192.168.88.1
dns,packet id:b14 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in 13-
Aug 14:52:21.32 from 192.168.88.1
dns,packet question: 1.0.0.127.dnsbugtest.1.0.0.127.in-
addr.arpa:PTR:IN in 13-Aug 14:52:21.32 from 192.168.88.1
dns query from 192.168.88.11: #4374
1.0.0.127.dnsbugtest.1.0.0.127.in-addr.arpa. PTR in 13-Aug
14:52:21.32 from 192.168.88.1
dns,packet --- sending udp query to 8.8.8.8:53: in 13-Aug
14:52:21.32 from 192.168.88.1
dns,packet id:782c rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 14:52:21.32 from 192.168.88.1
dns,packet question: 1.0.0.127.dnsbugtest.1.0.0.127.in-
addr.arpa:PTR:IN in 13-Aug 14:52:21.33 from 192.168.88.1
dns,packet --- got answer from 8.8.8.8:53: in 13-Aug 14:52:21.33
from 192.168.88.1
dns,packet id:782c rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 14:52:21.33 from 192.168.88.1
dns,packet question: 1.0.0.127.dnsbugtest.1.0.0.127.in-
addr.arpa:PTR:IN in 13-Aug 14:52:21.33 from 192.168.88.1
dns,packet answer: in 13-Aug 14:52:21.33 from 192.168.88.1
dns,packet <1.0.0.127.dnsbugtest.1.0.0.127.in-
addr.arpa:A:141=36.86.63.180> in 13-Aug 14:52:21.33 from
192.168.88.1
```

```
dns,packet authority: in 13-Aug 14:52:21.33 from 192.168.88.1
dns,packet <0.0.127.in-addr.arpa:SOA:86238=serial:1997022700
refresh:28800 retry:14400 expire:3600000 min:86400 > in 13-Aug
14:52:21.33 from 192.168.88.1
dns done query: #4374 dns name exists, but no appropriate record
in 13-Aug 14:52:21.33 from 192.168.88.1
dns,packet --- sending reply to 192.168.88.11:49152: in 13-Aug
14:52:21.33 from 192.168.88.1
dns,packet id:b14 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in 13-
Aug 14:52:21.33 from 192.168.88.1
dns,packet question: 1.0.0.127.dnsbugtest.1.0.0.127.in-
addr.arpa:PTR:IN in 13-Aug 14:52:21.33 from 192.168.88.1
dns,packet answer: in 13-Aug 14:52:21.33 from 192.168.88.1
dns,packet <1.0.0.127.dnsbugtest.1.0.0.127.in-
addr.arpa:A:141=36.86.63.180> in 13-Aug 14:52:21.33 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:34393->8.8.8.8:53, len 89 in 13-Aug 14:52:21.41 from
192.168.88.1
dns,packet --- got query from 192.168.66.20:59373: in 13-Aug
14:52:24.67 from 192.168.88.1
dns,packet id:34d3 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 14:52:24.68 from 192.168.88.1
dns,packet question: clients1.google.com:A:IN in 13-Aug
14:52:24.68 from 192.168.88.1
dns query from 192.168.66.20: #4375 clients1.google.com. A in 13-
Aug 14:52:24.68 from 192.168.88.1
dns,packet --- sending udp query to 8.8.8.8:53: in 13-Aug
14:52:24.68 from 192.168.88.1
dns,packet id:bc8e rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 14:52:24.68 from 192.168.88.1
dns,packet question: clients1.google.com:A:IN in 13-Aug
14:52:24.68 from 192.168.88.1
dns,packet --- got answer from 8.8.8.8:53: in 13-Aug 14:52:24.68
from 192.168.88.1
dns,packet id:bc8e rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 14:52:24.68 from 192.168.88.1
dns,packet question: clients1.google.com:A:IN in 13-Aug
14:52:24.68 from 192.168.88.1
dns,packet answer: in 13-Aug 14:52:24.68 from 192.168.88.1
dns,packet <clients1.google.com:CNAME:169=clients.l.google.com> in
13-Aug 14:52:24.68 from 192.168.88.1
dns,packet <clients.l.google.com:A:276=74.125.200.113> in 13-Aug
14:52:24.68 from 192.168.88.1
dns,packet <clients.l.google.com:A:276=74.125.200.138> in 13-Aug
14:52:24.68 from 192.168.88.1
dns,packet <clients.l.google.com:A:276=74.125.200.102> in 13-Aug
14:52:24.68 from 192.168.88.1
dns,packet <clients.l.google.com:A:276=74.125.200.139> in 13-Aug
14:52:24.68 from 192.168.88.1
dns,packet <clients.l.google.com:A:276=74.125.200.100> in 13-Aug
14:52:24.69 from 192.168.88.1
dns,packet <clients.l.google.com:A:276=74.125.200.101> in 13-Aug
14:52:24.69 from 192.168.88.1
dns done query: #4375 clients1.google.com 74.125.200.102 in 13-Aug
14:52:24.69 from 192.168.88.1
```

```
dns,packet --- sending reply to 192.168.66.20:59373: in 13-Aug
14:52:24.69 from 192.168.88.1
dns,packet id:34d3 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 14:52:24.69 from 192.168.88.1
dns,packet question: clients1.google.com:A:IN in 13-Aug
14:52:24.69 from 192.168.88.1
dns,packet answer: in 13-Aug 14:52:24.69 from 192.168.88.1
dns,packet <clients1.google.com:CNAME:169=clients.l.google.com> in
13-Aug 14:52:24.69 from 192.168.88.1
dns,packet <clients.l.google.com:A:279=74.125.200.102> in 13-Aug
14:52:24.69 from 192.168.88.1
dns,packet <clients.l.google.com:A:279=74.125.200.113> in 13-Aug
14:52:24.69 from 192.168.88.1
dns,packet <clients.l.google.com:A:279=74.125.200.138> in 13-Aug
14:52:24.69 from 192.168.88.1
dns,packet <clients.l.google.com:A:279=74.125.200.100> in 13-Aug
14:52:24.69 from 192.168.88.1
dns,packet <clients.l.google.com:A:279=74.125.200.139> in 13-Aug
14:52:24.69 from 192.168.88.1
dns,packet <clients.l.google.com:A:279=74.125.200.101> in 13-Aug
14:52:24.69 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:39719->8.8.8.8:53, len 65 in 13-Aug 14:52:24.77 from
192.168.88.1
dns,packet --- got query from 192.168.66.20:60243: in 13-Aug
14:52:24.88 from 192.168.88.1
dns,packet id:9887 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 14:52:24.88 from 192.168.88.1
dns,packet question: cdn.line-apps.com:A:IN in 13-Aug 14:52:24.88
from 192.168.88.1
dns query from 192.168.66.20: #4376 cdn.line-apps.com. A in 13-Aug
14:52:24.89 from 192.168.88.1
dns,packet --- sending udp query to 8.8.8.8:53: in 13-Aug
14:52:24.89 from 192.168.88.1
dns,packet id:5222 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 14:52:24.89 from 192.168.88.1
dns,packet question: cdn.line-apps.com:A:IN in 13-Aug 14:52:24.89
from 192.168.88.1
dns,packet --- got answer from 8.8.8.8:53: in 13-Aug 14:52:24.89
from 192.168.88.1
dns,packet id:5222 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 14:52:24.89 from 192.168.88.1
dns,packet question: cdn.line-apps.com:A:IN in 13-Aug 14:52:24.89
from 192.168.88.1
dns,packet answer: in 13-Aug 14:52:24.89 from 192.168.88.1
dns,packet <cdn.line-apps.com:CNAME:74185=cdn.line-
apps.com.edgesuite.net> in 13-Aug 14:52:24.89 from 192.168.88.1
dns,packet <cdn.line-apps.com.edgesuite.net:CNAME:435=cac-
cdn.line-apps.com.line-zero.akadns.net> in 13-Aug 14:52:24.90 from
192.168.88.1
dns,packet <cac-cdn.line-apps.com.line-
zero.akadns.net:CNAME:222=a1682.g.akamai.net> in 13-Aug
14:52:24.90 from 192.168.88.1
dns,packet <a1682.g.akamai.net:A:15=118.98.93.9> in 13-Aug
14:52:24.90 from 192.168.88.1
dns,packet <a1682.g.akamai.net:A:15=118.98.93.19> in 13-Aug
```

```
14:52:24.90 from 192.168.88.1
dns done query: #4376 cdn.line-apps.com 118.98.93.9 in 13-Aug
14:52:24.90 from 192.168.88.1
dns,packet --- sending reply to 192.168.66.20:60243: in 13-Aug
14:52:24.90 from 192.168.88.1
dns,packet id:9887 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 14:52:24.90 from 192.168.88.1
dns,packet question: cdn.line-apps.com:A:IN in 13-Aug 14:52:24.90
from 192.168.88.1
dns,packet answer: in 13-Aug 14:52:24.90 from 192.168.88.1
dns,packet <cdn.line-apps.com:CNAME:74185=cdn.line-
apps.com.edgesuite.net> in 13-Aug 14:52:24.90 from 192.168.88.1
dns,packet <cdn.line-apps.com.edgesuite.net:CNAME:435=cac-
cdn.line-apps.com.line-zero.akadns.net> in 13-Aug 14:52:24.90 from
192.168.88.1
dns,packet <cac-cdn.line-apps.com.line-
zero.akadns.net:CNAME:222=a1682.g.akamai.net> in 13-Aug
14:52:24.90 from 192.168.88.1
dns,packet <a1682.g.akamai.net:A:15=118.98.93.9> in 13-Aug
14:52:24.90 from 192.168.88.1
dns,packet <a1682.g.akamai.net:A:15=118.98.93.19> in 13-Aug
14:52:24.90 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto UDP, 192.168.66.20:59374-
>74.125.200.102:443, len 1378 in 13-Aug 14:52:24.96 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:49881->8.8.8.8:53, len 63 in 13-Aug 14:52:24.96 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:60253-
>118.98.93.9:80, len 52 in 13-Aug 14:52:24.96 from 192.168.88.1
dns,packet --- got query from 192.168.66.20:49880: in 13-Aug
14:52:27.89 from 192.168.88.1
dns,packet id:f904 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 14:52:27.89 from 192.168.88.1
dns,packet question: clients6.google.com:A:IN in 13-Aug
14:52:27.89 from 192.168.88.1
dns query from 192.168.66.20: #4377 clients6.google.com. A in 13-
Aug 14:52:27.89 from 192.168.88.1
dns,packet --- sending udp query to 8.8.8.8:53: in 13-Aug
14:52:27.89 from 192.168.88.1
dns,packet id:d084 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 14:52:27.89 from 192.168.88.1
dns,packet question: clients6.google.com:A:IN in 13-Aug
14:52:27.89 from 192.168.88.1
dns,packet --- got answer from 8.8.8.8:53: in 13-Aug 14:52:27.91
from 192.168.88.1
dns,packet id:d084 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 14:52:27.91 from 192.168.88.1
dns,packet question: clients6.google.com:A:IN in 13-Aug
14:52:27.91 from 192.168.88.1
dns,packet answer: in 13-Aug 14:52:27.91 from 192.168.88.1
dns,packet <clients6.google.com:CNAME:103=clients.l.google.com> in
13-Aug 14:52:27.91 from 192.168.88.1
dns,packet <clients.l.google.com:A:294=74.125.200.102> in 13-Aug
```

```
14:52:27.91 from 192.168.88.1
dns,packet <clients.l.google.com:A:294=74.125.200.113> in 13-Aug
14:52:27.91 from 192.168.88.1
dns,packet <clients.l.google.com:A:294=74.125.200.138> in 13-Aug
14:52:27.91 from 192.168.88.1
dns,packet <clients.l.google.com:A:294=74.125.200.100> in 13-Aug
14:52:27.91 from 192.168.88.1
dns,packet <clients.l.google.com:A:294=74.125.200.101> in 13-Aug
14:52:27.91 from 192.168.88.1
dns,packet <clients.l.google.com:A:294=74.125.200.139> in 13-Aug
14:52:27.91 from 192.168.88.1
dns done query: #4377 clients6.google.com 74.125.200.138 in 13-Aug
14:52:27.91 from 192.168.88.1
dns,packet --- sending reply to 192.168.66.20:49880: in 13-Aug
14:52:27.91 from 192.168.88.1
dns,packet id:f904 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 14:52:27.92 from 192.168.88.1
dns,packet question: clients6.google.com:A:IN in 13-Aug
14:52:27.92 from 192.168.88.1
dns,packet answer: in 13-Aug 14:52:27.92 from 192.168.88.1
dns,packet <clients6.google.com:CNAME:103=clients.l.google.com> in
13-Aug 14:52:27.92 from 192.168.88.1
dns,packet <clients.l.google.com:A:294=74.125.200.138> in 13-Aug
14:52:27.92 from 192.168.88.1
dns,packet <clients.l.google.com:A:294=74.125.200.100> in 13-Aug
14:52:27.92 from 192.168.88.1
dns,packet <clients.l.google.com:A:294=74.125.200.139> in 13-Aug
14:52:27.92 from 192.168.88.1
dns,packet <clients.l.google.com:A:294=74.125.200.101> in 13-Aug
14:52:27.92 from 192.168.88.1
dns,packet <clients.l.google.com:A:294=74.125.200.102> in 13-Aug
14:52:27.92 from 192.168.88.1
dns,packet <clients.l.google.com:A:294=74.125.200.113> in 13-Aug
14:52:27.92 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:55931->8.8.8.8:53, len 65 in 13-Aug 14:52:27.99 from
192.168.88.1
dns,packet --- got query from 192.168.66.20:56827: in 13-Aug
14:52:29.90 from 192.168.88.1
dns,packet id:8d12 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 14:52:29.90 from 192.168.88.1
dns,packet question: www.google.com:A:IN in 13-Aug 14:52:29.90
from 192.168.88.1
dns query from 192.168.66.20: #4378 www.google.com. A in 13-Aug
14:52:29.90 from 192.168.88.1
dns,packet --- sending udp query to 8.8.8.8:53: in 13-Aug
14:52:29.90 from 192.168.88.1
dns,packet id:d172 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 14:52:29.90 from 192.168.88.1
dns,packet question: www.google.com:A:IN in 13-Aug 14:52:29.91
from 192.168.88.1
dns,packet --- got answer from 8.8.8.8:53: in 13-Aug 14:52:29.91
from 192.168.88.1
dns,packet id:d172 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 14:52:29.91 from 192.168.88.1
dns,packet question: www.google.com:A:IN in 13-Aug 14:52:29.91
```

```
from 192.168.88.1
dns,packet answer: in 13-Aug 14:52:29.91 from 192.168.88.1
dns,packet <www.google.com:A:253=216.58.196.4> in 13-Aug
14:52:29.91 from 192.168.88.1
dns done query: #4378 www.google.com 216.58.196.4 in 13-Aug
14:52:29.91 from 192.168.88.1
dns,packet --- sending reply to 192.168.66.20:56827: in 13-Aug
14:52:29.91 from 192.168.88.1
dns,packet id:8d12 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 14:52:29.91 from 192.168.88.1
dns,packet question: www.google.com:A:IN in 13-Aug 14:52:29.91
from 192.168.88.1
dns,packet answer: in 13-Aug 14:52:29.94 from 192.168.88.1
dns,packet <www.google.com:A:253=216.58.196.4> in 13-Aug
14:52:29.94 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:46151->8.8.8.8:53, len 60 in 13-Aug 14:52:29.99 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:60254-
>216.58.196.4:443, len 52 in 13-Aug 14:52:29.99 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto UDP, 192.168.66.20:56828-
>216.58.196.4:443, len 1378 in 13-Aug 14:52:29.99 from
192.168.88.1
dns,packet --- got query from 192.168.66.20:55993: in 13-Aug
14:52:31.85 from 192.168.88.1
dns,packet id:d91e rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 14:52:31.88 from 192.168.88.1
dns,packet question: ad.doubleclick.net:A:IN in 13-Aug 14:52:31.89
from 192.168.88.1
dns query from 192.168.66.20: #4379 ad.doubleclick.net. A in 13-
Aug 14:52:31.91 from 192.168.88.1
dns,packet --- sending udp query to 8.8.8.8:53: in 13-Aug
14:52:31.95 from 192.168.88.1
dns,packet id:11e4 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 14:52:31.95 from 192.168.88.1
dns,packet question: ad.doubleclick.net:A:IN in 13-Aug 14:52:31.95
from 192.168.88.1
dns,packet --- got answer from 8.8.8.8:53: in 13-Aug 14:52:32.1
from 192.168.88.1
dns,packet id:11e4 rd:1 tc:0 aa:0 qr:1 ra:0 QUERY 'no error' in
13-Aug 14:52:32.8 from 192.168.88.1
dns,packet question: ad.doubleclick.net:A:IN in 13-Aug 14:52:32.8
from 192.168.88.1
dns,packet answer: in 13-Aug 14:52:32.8 from 192.168.88.1
dns,packet <ad.doubleclick.net:A:3600=74.125.200.148> in 13-Aug
14:52:32.8 from 192.168.88.1
dns,packet <ad.doubleclick.net:A:3600=74.125.200.149> in 13-Aug
14:52:32.9 from 192.168.88.1
dns,packet <ad.doubleclick.net:A:3600=216.58.221.70> in 13-Aug
14:52:32.9 from 192.168.88.1
dns done query: #4379 ad.doubleclick.net 74.125.200.148 in 13-Aug
14:52:32.9 from 192.168.88.1
dns,packet --- sending reply to 192.168.66.20:55993: in 13-Aug
14:52:32.9 from 192.168.88.1
```

```
dns,packet id:d91e rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 14:52:32.9 from 192.168.88.1
dns,packet question: ad.doubleclick.net:A:IN in 13-Aug 14:52:32.9
from 192.168.88.1
dns,packet answer: in 13-Aug 14:52:32.9 from 192.168.88.1
dns,packet <ad.doubleclick.net:A:3600=74.125.200.148> in 13-Aug
14:52:32.9 from 192.168.88.1
dns,packet <ad.doubleclick.net:A:3600=74.125.200.149> in 13-Aug
14:52:32.9 from 192.168.88.1
dns,packet <ad.doubleclick.net:A:3600=216.58.221.70> in 13-Aug
14:52:32.9 from 192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, proto UDP,
192.168.0.105:37805->8.8.8.8:53, len 64 in 13-Aug 14:52:32.9 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto UDP, 192.168.66.20:55994-
>74.125.200.148:443, len 1378 in 13-Aug 14:52:33.36 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto UDP, 192.168.66.20:55996-
>74.125.130.138:443, len 1378 in 13-Aug 14:52:34.27 from
192.168.88.1
firewall,info srcnat: in:(none) out:ether1-INET, src-mac
54:04:a6:79:c8:01, proto TCP (SYN), 192.168.66.20:60255-
>74.125.130.138:443, len 52 in 13-Aug 14:52:34.40 from
192.168.88.1
dns,packet --- got query from 192.168.88.11:54844: in 13-Aug
14:52:35.60 from 192.168.88.1
dns,packet id:c8fe rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 14:52:35.60 from 192.168.88.1
dns,packet question: 4-edge-chat.facebook.com:A:IN in 13-Aug
14:52:35.60 from 192.168.88.1
dns query from 192.168.88.11: #4380 4-edge-chat.facebook.com. A in
13-Aug 14:52:35.60 from 192.168.88.1
dns,packet --- sending udp query to 8.8.4.4:53: in 13-Aug
14:52:35.60 from 192.168.88.1
dns,packet id:f719 rd:1 tc:0 aa:0 qr:0 ra:0 QUERY 'no error' in
13-Aug 14:52:35.60 from 192.168.88.1
dns,packet question: 4-edge-chat.facebook.com:A:IN in 13-Aug
14:52:35.60 from 192.168.88.1
dns,packet --- got answer from 8.8.4.4:53: in 13-Aug 14:52:35.63
from 192.168.88.1
dns,packet id:f719 rd:1 tc:0 aa:0 qr:1 ra:1 QUERY 'no error' in
13-Aug 14:52:35.63 from 192.168.88.1
dns,packet question: 4-edge-chat.facebook.com:A:IN in 13-Aug
14:52:35.63 from 192.168.88.1
```

CURRICULUM VITAE

Identitas Diri

Nama	: Nugroho Febriansyah Putra
Tempat/ Tanggal Lahir	: Pacitan, 28 Februari 1991
Jenis Kelamin	: Laki - laki
Status Perkawinan	: Belum Menikah
Tinggi/ Berat Badan	: 183CM / 83KG
Golongan Darah	: B
Alamat Jogja	: Jalan Jawa Nomor 26 Rt 09 Rw 25 Widorobaru Ngropoh Condongcatur Depok Sleman Yogyakarta 55283
Pendidikan Terakhir	: Mahasiswa Universitas Islam Negeri Sunan Kalijaga
Email	: nugroho.febriansyah@student.uin-suka.ac.id dowo314@gmail.com
Telepon	: 085749192254

Pendidikan

TAHUN	JENJANG PENDIDIKAN
1995 - 1997	TK BHAYANGKARA PACITAN
1997 - 2003	SD N BALEHARJO II PACITAN
2003 - 2006	SMP N 3 PACITAN
2006 - 2009	SMK N 1 PACITAN
2009 - 2016	UIN SUNAN KALIJAGA YOGYAKARTA

Pengalaman Kerja / Magang

TAHUN	JENJANG KERJA / MAGANG
2008	GROSCOM DISTRIBUTOR MONITOR YOGYAKARTA
2009	DUTA NIAGA II COMPUTER
2010	OPERATOR / TEKNISI JAVA WARNET
2012	TEKNISI LAB SAINS DAN TEKNOLOGI UIN-SUKA
2013	TARGET SECURINDO SECURITY / SOUNDRENALINE
2016	TEKNISI PT. INFORMATION TECHNOLOGY SERVICE CENTRE YOGYAKARTA