ANALISIS KEAMANAN SISTEM INFORMASI BERDASARKAN STANDAR ISO 27001 PADA JARINGAN KLINIK PRATAMA UIN SUNAN KALIJAGA YOGYAKARTA

Skripsi

Untuk memenuhi sebagian persyaratan

mencapai derajat Sarjana S-1

Program Studi Teknik Informatika

Disusun oleh:

Ferdian Noor Pambudi

12650025

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2019

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274).540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-3005/Un.02/DST/PP.00.9/08/2019

Tugas Akhir dengan judul : ANALISIS KEAMANAN SISTEM INFORMASI BERDASARKAN STANDAR ISO 27001 PADA JARINGAN KLINIK PRATAMA UIN SUNAN KALIJAGA YOGYAKARTA

yang dipersiapkan dan disusun oleh:

Nama	: FERDIAN NOOR PAMBUDI
Nomor Induk Mahasiswa	: 12650025
Telah diujikan pada	: Rabu, 31 Juli 2019
Nilai ujian Tugas Akhir	: A/B

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

TIM UJIAN TUGAS AKHIR

Ketua Sidang

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

Penguji I

Maria Ulfah Siregar, S.Kom. MIT., Ph.D.
NIP. 19780106 200212 2 001

Penguji II

Nurochman, S.Kom., M.Kom
NIP. 19801223 200901 1 007

Yogyakarta, 31 Juli 2019
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Plh. Dekan

Dr. Agung Fatwanto, S.Si., M.Kom.
NIP. 19770103 200501 1 003

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Permohonan
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 : Ferdian Noor Pambudi
NIM : 12650025
Judul Skripsi : Analisis Keamanan Sistem Informasi Berdasarkan Standar ISO 27001 Pada Jaringan Klinik Pratama UIN Sunan Kalijaga Yogyakarta

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

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, 26 Juli 2019
Pembimbing

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

PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini:

Nama	: Ferdian Noor Pambudi
NIM	: 12650025
Program Studi	: Teknik Informatika
Fakultas	: Sains dan Teknologi

Menyatakan bahwa skripsi dengan judul " **Analisis Keamanan Sistem Informasi Berdasarkan Standar ISO 27001 Pada Jaringan Klinik Pratama UIN Sunan Kalijaga Yogyakarta** " tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 26 Juli 2019

Yang Menyatakan

Ferdian Noor Pambudi
NIM. 12650025

KATA PENGANTAR

Bismillahirrahmanirrahim, puji syukur atas kehadirat Allah SWT yang telah melimpahkan rahmat, hidayah serta inayah-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Analisis Keamanan Sistem Informasi Berdasarkan ISO 27001 Pada Jaringan Klinik Pratama UIN Sunan Kalijaga" ini dengan baik sesuai dengan kewajiban dalam memenuhi gelar Strata 1 Komputer (S.Kom) di Jurusan Teknik Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Tidak lupa shalawat serta salam tetap tercurah kepada junjungan Nabi Muhammad SAW dan semoga kelak kita mendapat syafaat darinya.

Oleh karena itu, penulis ingin mengucapkan terima kasih sebesar-besarnya kepada:

1. Bapak Prof. Drs. K.H. Yudian Wahyudi, M.A., Ph.D. selaku Rektor Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
2. Bapak Dr. Murtono, M.Si., selaku Dekan Fakultas Sains dan Teknologi UIN Sunan Kalijaga.
3. Bapak Sumarsono, S.T., M.Kom., selaku Ketua Program Studi Teknik Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta serta Dosen Pembimbing skripsi yang telah memberikan arahan, saran, waktu serta masukan kepada penulis dalam menyusun skripsi.
4. Bapak Aulia Faqih Rifa'i, M.Kom., selaku dosen pembimbing akademik kelas reguler Teknik Informatika 2012.
5. Bapak Nurochman, S.Kom., M.Kom dan Ibu Maria Ulfah Siregar, S.Kom. MIT., Ph.D., selaku penguji dan pemberi perbaikan dalam penyusunan skripsi penulis.
6. Bapak dan Ibu Dosen Program Studi Informatika UIN Sunan Kalijaga yang telah memberikan banyak bekal ilmu kepada penulis.
7. Ibu Dr. Diana Rismajani selaku Kepala Klinik Pratama UIN Sunan Kalijaga yang telah memberikan izin penelitian.

8. Bapak Alfian selaku pemberi arahan dan narasumber kepada penulis sewaktu penyusunan skripsi
9. Orang tua dan keluarga tercinta yang senantiasa memberikan motivasi serta dukungan baik moril maupun materiil kepada penulis dengan semua kasih sayangnya.
10. Teman-teman Teknik Informatika yang tidak dapat disebutkan satu persatu yang telah memberikan bantuan, dukungan, serta motivasi kepada penulis.
11. Semua pihak yang telah memberikan bantuan dan dukungan selama menempuh strata satu teknik informatika khususnya dalam penyusunan skripsi ini yang tidak dapat disebut satu persatu. Terima kasih.

Semoga Allah SWT membalas amal kebaikan dari seluruh pihak yang telah membantu penulis menyelesaikan skripsi. Penulis menyadari sepenuhnya masih banyak kesalahan dan kekurangan dalam skripsi ini, maka dari itu berbagai saran dan kritik sangat diharapkan demi perbaikan. Semoga skripsi ini dapat bermanfaat bagi penyusun sendiri pada khususnya dan bagi para pembaca pada umumnya. Terima kasih.

Yogyakarta, 9 Agustus 2019

Penulis

HALAMAN PERSEMBAHAN

Alhamdulillah segala doa dan syukur tiada henti terucap kehadirat Allah SWT, Tuhan seluruh alam semesta. Shalawat serta salam kepada junjungan Nabi Muhammad SAW semoga senantiasa kita kelak mendapat syafaat darinya dan menjadi umat yang bertaqwa. Saya persembahkan kepada orang-orang yang telah membantu saya dalam menyelesaikan skripsi ini baik berupa dukungan moral maupun spiritual:

1. Kedua Orang tua, Dra.Ismulyani dan Drs.Budiyono.
2. Kakak-kakak perempuan dan Adik laki-lakiku tersayang, Findhy Listiyaning Putri, Fitria Cahyaning Putri, Listia Fatmajati Pertiwi dan Fanandi Agung Pambudi.
3. Teman – teman yang selalu memberikan dukungan dalam pembuatan skripsi A.S Wahid Faizin, Alfian Gautama H., M. Murah Pamuji, Alif Aziz, M. Dzulfikar Fauzi, Wahib Ramadhan, Sulton Daud Ul Mukarobin, Alfian Nur Jayanto, Anwaruddin Kamal Ibrahim.
4. Teman-teman Teknik Informatika 2012
5. Teman-teman satu kost INOMI

HALAMAN MOTTO

Tidak ada kata sia-sia dalam hal mencoba dan tidak ada kesuksessan tanpa mencoba.

When you have never made a mistake, it means you have not tried anything.

Do or D.O

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

ANALISIS KEAMANAN SISTEM INFORMASI BERDASARKAN STANDAR ISO 27001 PADA JARINGAN KLINIK PRATAMA UIN KALIJAGA YOGYAKARTA

Ferdian Noor Pambudi
12650025

INTISARI

Penelitian ini dilakukan untuk menganalisis tingkat kematangan keamanan sistem informasi serta keamanan jaringan pada Klinik Pratama UIN Sunan Kalijaga Yogyakarta. Proses pengambilan data dilakukan dengan audit pada Sistem informasi dan Administrasi (SIMA) dengan klausul kebijakan keamanan, pengelolaan aset, keamanan fisik dan lingkungan, manajemen komunikasi dan operasi, serta pengendalian akses berdasarkan ISO 27001, kemudian dilakukan pengujian keamanan jaringan dengan melakukan pengujian penyerangan pada jaringan komputer yang diterapkan di Klinik Pratama UIN Sunan Kalijaga.

Data yang dianalisis berupa data kusioner yang diperoleh dari hasil wawancara pihak pengurus Sistem Informasi dan Administrasi (SIMA) di Klinik Pratama sesuai dengan klausul dengan pendekatan *Maturity level*. Sedangkan data yang dianalisis untuk keamanan jaringan, diperoleh dengan melakukan pengujian penyerangan (*penetration testing)* dari tahapan *information gathering, vunerability assessment* dan *spoofing*.

Hasil penelitian ini menunjukkan bahwa tingkat keamanan dari Sistem Informasi dan Administrasi (SIMA) Klinik Pratama UIN Sunan Kalijaga berdasarkan klausul kebijakan keamanan, pengelolaan aset, keamanan fisik dan lingkungan, manajemen komunikasi dan operasi dan pengendalian akses menurut ISO 27001 berada pada skala kematangan 2,288 (*Repeatable but Intuitive*). Sedangkan pada keamanan jaringannya tidak rentan atau aman karena pada serangan MitM (*Man in the Middle Attack*) menggunakan ARP *Poisoning* tidak berhasil masuk ke jaringan komputer di Klinik Pratama UIN Sunan Kalijaga.

Kata Kunci : Klinik Pratama UIN Sunan Kalijaga, Sistem Informasi dan Administrasi (SIMA), ISO 27001, pengujian penyerangan.

SECURITY ANALYSIS OF INFORMATION SYSTEM PRATAMA CLINIC UIN SUNAN KALIJAGA YOGYAKARTA NETWORK BASED ON ISO 27001 STANDARDS

Ferdian Noor Pambudi
12650025

ABSTRACT

This research was conducted to analyze the maturity level of information system security and network security at the Pratama Clinic UIN Sunan Kalijaga Yogyakarta. Data retrieval process is carried out by auditing the Information and Administration System (SIMA) with clauses of security policy, asset management, physical and environmental security, communication and operations management, and access control based on ISO 27001, then network security testing is carried out by testing assault on the computer network that is applied at the Pratama Clinic UIN Sunan Kalijaga.

Data analyzed in the form of questionnaire, data obtained from interviews with the management of the Information and Administration System (SIMA) in the Pratama Clinic in accordance clauses with the Maturity level approach. While the data analyzed for network security, obtained by conducting assault testing (penetration testing) from stages of information gathering, vunerability assessment and spoofing.

The results of this study indicate that the security level of the Information and Administration System (SIMA) of the Pratama Clinic UIN Sunan Kalijaga based on clauses of security policy, asset management, physical and environmental security, communication and operation management and access control according to ISO 27001 are on a maturity scale of 2.262 (Repeatable but Intuitive). Whereas the network security is not vulnerable or secure because the MitM (Man in the Middle Attack) attack using ARP Poisoning did not make it into the computer network at the Pratama Clinic UIN Sunan Kalijaga.

Keywords: Pratama Clinic UIN Sunan Kalijaga, Information and Administration System (SIMA), ISO 27001, assault testing

BAB I
PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi informasi (*information technology*) yang cepat, membuat persaingan antar perusahaan semakin besar dalam perberian layanannya. Hal ini dikarenakan teknologi informasi dapat membantu manusia dalam membuat, mengubah, menyimpan, mengomunikasikan dan/atau menyebarkan informasi sehingga meningkatkan produktivitas kerja pada suatu proses bisnis dalam sebuah perusahaan.

Sistem informasi merupakan salah satu teknologi informasi yang digunakan suatu perusahaan untuk mendukung operasi dan manajemen dalam membantu untuk mengontrol kinerja proses bisnis serta bertujuan menghasilkan data yang relevan (*relevance*), tepat waktu (*timeliness*), dan akurat (*accurate*). Perlindungan data-data dalam sistem informasi tersebut harus dilakukan agar resiko dari pihak yang tidak bertanggungjawab dapat memanfaatkan kerentanan pada sistem informasi untuk mengambil keuntungan dari data tersebut. Keamanan sistem informasi merupakan suatu cara yang digunakan untuk memberikan perlindungan agar terhindar dari berbagai ancaman luar seperti pencurian data dan kebocoran informasi. Selain itu pengujian keamanan jaringan pada perusahaan juga perlu dilakukan untuk mengetahui kerentanan yang mungkin bisa di akses oleh pihak yang tidak bertanggung jawab.

Klinik Pratama UIN Sunan Kalijaga Yogyakarta adalah salah satu pelayanan kesehatan yang telah menerapakan sistem informasi dalam melayani para pasiennya. Sistem informasi yang diterapkan tersebut menggunakan aplikasi pada jaringan lokal yang saling terhubung antar komputer dengan server (*client-server*) yang disebut Sistem Informasi dan Administrasi (SIMA).

Keamanan sistem informasi sangatlah penting untuk melindungi data dan sistem yang ada, sehingga apapun bentuk informasi yang disajikan, informasi tersebut harus selalu terjaga dan aman. Mengingat pentingnya keamanan informasi pada suatu jaringan, untuk itu perlu dilakukan audit untuk mengetahui bagaimana kebijakan keamanan informasi yang diterapkan oleh pengelola sistem informasi dan administrasi Klinik Pratama UIN Sunan Kalijaga, seperti apa kebijakan keamanan, pengelolaan aset, keamanan fisik dan lingkungannya, bagaimana bentuk manajemen komunikasi dan operasi serta pengendalian akses serta pengujian keamanan jaringan pada sistemnya.

Dilakukannya audit keamanan sistem informasi dan pengujian jaringan pada Klinik Pratama UIN Sunan Kalijaga dapat menghasilkan hasil dari audit keamanan sistem informasi berupa pernyataan, pertanyaan, jawaban, hasil perhitungan *maturity level*, serta rekomendasi hasil penelitian dan hasil dari pengujian keamanan jaringan berupa informasi jaringan, kerentanan jaringan, penyerangan jaringan, serta rekomendasi hasil pengujian. Hasil analisis ini dapat dijadikan sebagai acuan dalam mengukur ketepatan sistem informasi dengan keamanan jaringan yang diterapkan. Selain itu, hasil temuan nantinya akan dianalisis menjadi sebuah rekomendasi yang ditujukan untuk organisasi. Dengan adanya rekomendasi tersebut, organisasi dapat menjadikan acuan dalam mengambil keputusan untuk memperbaiki sistem yang diterapkan.

ISO 27001 merupakan sebuah seri perpaduan prinsip – prinsip yang berfungsi untuk menginisiasi, implementasi, pemeliharaan dan meningkatkan kinerja manajemen teknologi informasi dalah sebuah organisasi IT. ISO 27001 merupakan standar yang diakui secara internasional karena memiliki cara yang baik di bidang keamanan. ISO 27001 juga merupakan dokumen standar Sistem Manajemen Keamanan Informasi (SMKI) atau *Information Security Management Systems* (ISMS) yang memberikan gambaran secara umum mengenai apa saja yang seharusnya dilakukan dalam usaha pengimplementasian konsep – konsep keamanan informasi.

Standar yang digunakan dalam audit keamanan sistem informasi pada Klinik Pratama UIN Sunan Kalijaga adalah ISO 27001. Standar ini dipilih karena sangat fleksibel untuk dikembangkan berdasarkan dari kebutuhan suatu lembaga atau organisasi, tujuan organisasi, persyaratan keamanan, proses bisnis dan jumlah pegawai serta ukuran struktur organisasi.

Berdasarkan uraian di atas maka penulis ingin melakukan analisis dan pengujian dengan permasalahan tersebut sebagai bahan penelitian ini. Penulis berharap dapat menghasilkan dokumen (temuan dan rekomendasi) yang merupakan hasil audit keamanan sistem informasi dan hasil analisis pengujian keamanan jaringan. Adapun judul untuk penelitian ini yaitu "Analisis Keamanan Sistem Informasi Berdasarkan ISO 27001 Pada Jaringan Klinik Pratama UIN Sunan Kalijaga".

1.2. Rumusan Masalah

Berdasarkan penjelasan pada latar belakang, maka perumusan masalah yang didapat adalah sebagai berikut :

1. Bagaimana melaksanakan analisis Sistem Informasi dan Administrasi Klinik Pratama UIN Sunan Kalijaga berdasarkan standar ISO 27001?
2. Bagaimana hasil analisis Sistem Informasi dan Administrasi Klinik Pratama UIN Sunan Kalijaga berdasarkan standar ISO 27001?
3. Bagaimana melaksanakan analisis Keamanan Jaringan Klinik Pratama UIN Sunan Kalijaga dengan *penetration testing*?
4. Bagaimana menyusun hasil analisis Keamanan Jaringan Klinik Pratama UIN Sunan Kalijaga dengan *penetration testing*?

1.3. Batasan Masalah

Batasan masalah dalam penelitian ini adalah sebagai berikut :

1. Sistem Informasi yang dianalisis adalah Sistem Informasi dan Administrasi (SIMA) yang diterapkan oleh Klinik Pratama UIN Sunan Kalijaga.
2. Keamanan Jaringan yang dianalisis dengan *penetration testing* adalah topologi jaringan yang diterapkan oleh Klinik Pratama UIN Sunan Kalijaga.

3. *Penetration testing* dilakukan menggunakan *tools*: traceroute, Ipconfig, Ifconfig untuk mendapatkan/melakukan *Information Gathering* pada jaringan komputer dan laptop (Kali Linux) , Nmap dan Zenmap untuk mengetahui celah keamanan dan topologi jaringan komputer, menggunakan Wireshark untuk mengetahui kerentanan pada protokol komputer maupun *internet*, serta *tool* Ettercap untuk serangan MITMS pada jaringan komputer di Klinik Pratama UIN Yogyakarta.
4. Analisis dilakukan menggunakan standar ISO 27001.
5. Data yang digunakan dalam analisis dan pembahasan masalah adalah data yang diperoleh dari *penetration testing*, observasi dan wawancara.
6. Analisis yang digunakan adalah metode penilaian (*scoring*) dengan pendekatan sesuai standar ISO 27001 yaitu model *maturity level.*
7. Klausul yang digunakan yaitu:
   a. Kebijakan keamanan
   b. Pengelolaan aset
   c. Keamanan fisik dan lingkungan
   d. Manajemen komunikasi dan operasi
   e. Pengendalian akses
8. *Output* yang dihasilkan dalam penelitian ini adalah penilaian dan rekomendasi Sistem Informasi serta Keamanan Jaringan Klinik Pratama UIN Sunan Kalijaga
9. Bagaimana mengetahui gap antara hasil analisis keamanan jaringan dan hasil audit Sistem Informasi dan Administrasi (SIMA) Klinik Pratama UIN Sunan Kalijaga.

1.4. Tujuan Penelitian

Tujuan dari penelitian ini adalah :

1. Mendapatkan hasil pengukuran Keamanan Sistem Informasi Klinik Pratama UIN Sunan Kalijaga sesuai standar ISO 27001.
2. Menyusun hasil analisis Keamanan Sistem Informasi Klinik Pratama UIN Sunan Kalijaga berdasarkan standar ISO 27001.
3. Mengetahui kerentanan pada Keamanan Jaringan Klinik Pratama UIN Sunan Kalijaga menggunakan metode *penetration testing*.
4. Melaporkan hasil kerentanan pada Keamanan Jaringan Klinik Pratama UIN Sunan Kalijaga berdasarkan hasil *penetration testing.*

1.5. Manfaat Penelitian

Hasil penelitian ini diharapkan dapat memberikan manfaat baik secara teoritis maupun praktis, yaitu sebagai berikut:

1. Manfaat Teoritis

   Penelitian ini diharapkan dapat menjadi acuan bagi penelitian sejenis dan bagi peneliti diharapkan dapat bermanfaat dalam menambah pengetahuan dan wawasan terutama dalam hal yang sesuai dengan penelitian yang dikaji peneliti yaitu analisis Keamanan Sistem Informasi berdasarkan standar ISO 27001 pada Jaringan Klinik Pratama UIN Sunan KalijagaYogyakarta.

2. Manfaat Praktis

   a) Dengan melakukan penelitian ini diharapkan dapat menjadikan suatu bahan kajian yang nantinya dapat meningkatkan mutu program studi Teknik Informatika Universitas Islam Negeri Sunan Kalijaga Yogyakarta tempat penulis memperoleh ilmu.

   b) Pihak-pihak lain yang berhubungan dengan bidang komputer terutama yang berhubungan dengan analisis keamanan jaringan berdasarkan ISO 27001 yang memerlukan hasil dari penelitian ini.

1.6. Kontribusi Penelitian

Penelitian ini dapat dijadikan sebagai bahan kajian yang nantinya dapat dikembangkan untuk meningkatkan mutu pendidikan.

1.7. Sistematika Penulisan

Sistematika penulisan skripsi ini dibuat untuk memberikan gambaran secara garisbesar tentang penelitian yang dilakukan penulis. Sistematika penulisan skripsi ini adalah sebagai berikut :

BAB I. PENDAHULUAN

Pada bagian bab ini membahas tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, kontribusi penelitian

BAB II TINJAUAN PUSTAKA DAN LANDASAN TEORI

Pada bagian bab ini berisi tentang tinjauan pustaka dan landasan teori yang berhubungan dengan topik yang akan dibahas dalam penelitian ini.

BAB III METODE PENELITIAN

Pada bagian bab ini berisi tentang uraian rinci tentang metode penelitian yang memberikan penjelasan mengenai detail langkah-langkah yang dilakukan untuk mencapai tujuan dan kesimpulan akhir penelitian.

BAB IV HASIL DAN PEMBAHASAN

Pada bagian bab ini berisi tentang Perancangan Audit, Proses Audit, Analisis dan Hasil Audit, Hasil Audit dan Rekomendasi, Hasil dan Pembahasan Penetration Testing dan Rekomendasi, Gap Analisis.

BAB V KESIMPULAN DAN SARAN

Pada bagian bab ini berisi tentang Kesimpulan dan Saran dari hasil penelitian yang dilakukan

DAFTAR PUSTAKA

Pada bagian ini berisi tetang reverensi-reverensi yang digunakan penulis dalam penyusunan dan pelaksanaan penelitian.

LAMPIRAN

Pada bagian bab ini berisi bukti-bukti gambar dari hasil audit dan *penetration testing*.

BAB V
KESIMPULAN

5.1 Kesimpulan

Berdasarkan hasil penelitian yang dilakukan mulai dari perencanaan hingga didapatkannya hasil penelitian, maka kesimpulan yang peneliti hasilkan dari proses audit Sistem Informasi dan Administrasi serta Keamanan Jaringan pada Klinik Pratama UIN Sunan Kalijaga adalah sebagai berikut:

1) Hasil analisis pengukuran Keamanan Sistem Informasi dan Adminstrasi (SIMA) Klinik Pratama UIN Sunan Kalijaga berdasarkan standar ISO 27001 pada klausul kebijakan keamanan dengan nilai *maturity* sebesar 1,2 (*Initial / Ad Hoc*), klausul pengelolaan aset dengan nilai *maturity* sebesar 3,07 (*Defined Process*), klausul keamanan fisik dan lingkungan dengan nilai *maturity* sebesar 2,00 (*Repeatable but Intuitive*), klausul manajemen komunikasi dan operasi dengan nilai *maturity* sebesar 2,17 (*Repeatable but Intuitive*) serta klausul pengendalian akses dengan nilai *maturity* sebesar 3,00 (*Defined Process*).

2) Setelah melakukan proses analisis terhadap hasil audit yang didapatkan dari klausul kebijakan keamanan, pengelolaan aset, keamanan fisik dan lingkungan, manajemen komunikasi dan operasi, serta pengendalian akses, diperoleh nilai *maturity* sebesar 2,288 dengan *maturity level Repeatable but Intuitive.*

3) Metode *penetration testing* yang dilakukan penulis pada keamanan jaringan Klinik Pratama UIN Sunan Kalijaga terdiri dari tahap *information gathering, vunerability assessment,* dan *spoofing.* Pada tahap *information gathering tools* yang digunakan adalah ipconfig, ifconfig, dan traceroute. Pada tahap *vunerability assessment tools* yang digunakan adalah Nmap dan Zenmap. Sedangkan pada tahap *spoofing tools* yang digunakan adalah Wireshark dan Ettercap.

4) Hasil kerentanan pada Keamanan Jaringan Klinik Pratama UIN Sunan Kalijaga berdasarkan tahapan metode *penetration testing* adalah pada tahapan *information gathering* didapatkan alamat-alamat ip dan jalur pengiriman data yang terhubung pada jaringan komputer (Dell-PC dan laptop Kali Linux). Pada tahap *vunerability assessment* didapatkan *port-port* yang terbuka di Dell-PC dan laptop Kali Linux yaitu *port* 22, 53,80, 443 (*tcpwrapped*), 8888, 443 (http) pada Dell-PC sedangkan *port* 22, , 23, 80, 135, 139, 443, 445, 49152-49163, 2869, 5357, 6646 pada laptop Kali Linux. Dan pada tahap *spoofing* didapatkan protokol –protokol *internet* rentan terhadap pembacaan paket data yaitu *protocol* HTTP dan SSDP, serta pada percobaan penyerangan MitM dengan ARP *Poisoning* pada jaringan komputer *target* tidak berhasil masuk. Dapat disimpulkan bahwa Keamanan Jaringan Klinik Pratama cukup aman.

5.2 Saran

Dari semua proses yang telah dilakukan oleh peneliti, tentunya masih terdapat beberapa hal yang harus di perbaiki dan ditingkatkan. Oleh karena itu untuk penelitian lebih lanjut, peneliti memberikan saran berupa masukan sebagai berikut:

1) Sebaiknya dilakukan audit internal menggunakan standar ISO 27001 secara rutin oleh pengelola agar mengetahui berapa tingkat kematangan keamanan Sistem Informasi dan Administrasi Klinik Pratama UIN Sunan Kalijaga serta pemeliharaan kabel-kabel jaringan komputer agar dapat memberikan pengaruh yang signifikan atas keberlangsungan pelayanan yang ada di Klinik tersebut.

2) Diharapkan untuk penelitian lebih lanjut mengenai Sistem Informasi dan Administrasi Klinik Pratama UIN Sunan Kalijaga dapat menggunakan klausul secara keseluruhan yang ada pada ISO 27001 karena dapat memperoleh nilai kematangan yang menyeluruh dalam proses pengelolaan Sistem Informasi yang semakin akurat.

3) Penelitian selanjutnya diharapkan menambahkan teknik *penetration testing* yang lain karena seiring berkembangnya teknologi tidak menutup kemungkinan bermunculannya teknik – teknik serangan yang bisa menembus jaringan pada sistem informasi tersebut.

DAFTAR PUSTAKA

Anggraini, Lusi.2016. *Audit Keamanan Sistem Informasi Perpustakaan Kota Yogyakarta Berdasarkan Standar ISO 27001.* Yogyakarta : Skripsi UIN Sunan Kalijaga.

Garfinkel, Simson. 1995. *Pretty Good Privacy*. USA: O'Reilly & Associates, Inc.

Heri, Setiawan.2015. *Audit Sistem Informasi Rumah Sakit Menggunakan Standart ISO 27001 (Studi Kasus DI RSU PKU Muhammadiyah Bantul).* Yogyakarta : Skripsi UIN Sunan Kalijaga.

Howard, John D. 1997. *An Analysis Of Security Incidents On The Internet 1989 – 1995*. Pittsburg: PhD thesis Carnegie Mellon University.

Iffano, Irsyat dan Sarno, Riyanarto.2009. *Sistem Manajemen Keamanan Informasi*. Surabaya : ITS Press.

Juhdan.2016. *Audit Keamanan Sistem Informasi Digital Library Universitas Islam Negeri Sunan Kalijaga Menggunakan Standar SNI - ISO 27001*. Yogyakarta : Skripsi UIN Sunan Kalijaga.

Kristanto, Titus ; ARIEF, Rachman; ROZI, Nanang Fakhrur. 2014. *Perancangan Audit Keamanan Informasi Berdasarkan Standar Iso 27001: 2005 (Studi Kasus: Pt Adira Dinamika Multi Finance)*. Surabaya : SESINDO.

Mulyana, Y. B.2002. *Linux Semudah Windows*. Jakarta : PT. Elex Media Komputindo.

Muniz, J., & Lakhani, A.2013. *Web Penetration Testing with Kali Linux*. Packt Publishing.

Nasional, Direktorat Badan Standarisasi. SNI ISO/IEC 27001. 2009. *Teknologi Informasi-Teknik Keamanan-Sistem Manajemen Keamanan Informasi-Persyaratan*. Jakarta*:* Badan Standardisasi Nasional–BSN.

Permatasari, D.I.2016. *Audit Keamanan Informasi Berdasarkan Standar SNI-ISO 27001 Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogyakarta*. Yogyakarta: Skripsi UIN Sunan Kalijaga.

Sarno, Riyanarto. 2009. *Audit Sistem dan Teknologi Informasi*. Surabaya*:* ITS Press.

Tata Sutabri.2005. *Sistem Informasi Manajemen.* Yogyakarta : Andi.

Trismiati, Ika.2018. *Analisis Keamanan Jaringan Menggunakan Standar ISO 27001 Pada PTIPD (Pusat Teknologi Informasi dan Pangkalan Data) UIN Sunan Kalijaga Yogyakarta.* Yogyakarta: Skripsi UIN Sunan Kalijaga

Wecan, P.P. 2017. *Pengujian Kamanan Sistem Informasi Akademik Universitas Islam Negeri Sunan Kalijaga Yogyakarta*. Yogyakarta: Skripsi UIN Sunan Kalijaga.

LAMPIRAN

LAMPIRAN 1

Tabel Sasaran Pengendalian SNI-ISO 27001

Klausul	Kontrol	Pengendalian / Sasaran
A.5	SNI-ISO 27001 A.5.1 Kebijakan Keamanan Informasi	Memberikan arahan dan dukungan manajemen untuk keamanan informasi menurut persyaratan bisnis dan hukum beserta regulasi yang relevan
A.6	SNI-ISO 27001 A.6.1 Organisasi Keamanan Informasi (*internal*)	Mengelola keamanan informasi dalam organisasi
	SNI-ISO 27001 A.6.2 Organisasi Keamanan Informasi (*eksternal*)	Memelihara keamanan informasi organisasi dan fasilitas pengolahan informasi yang diakses, diolah, dikomunikasikan kepada atau dikelola pihak *eksternal*
A.7	SNI-ISO 27001 A.7.1 Pengelolaan Aset (tanggung jawab terhadap aset)	Mencapai dan memelihara perlindungan yang sesuai terhadap aset organisasi
	SNI-ISO 27001 A.7.2 Pengelolaan Aset (klasifikasi informasi)	Memastikan bahwa informasi menerima tingkat perlindungan yang tepat
A.8	SNI-ISO 27001 A.8.1 Keamanan Sumber Daya Manusia (sebelum dipekerjakan)	Memastikan bahwa pegawai, kontraktor, dan pengguna pihak ketiga memahami tanggung jawab sesuai dengan perannya, dan untuk mengurangi resiko pencurian, kecurangan atau penyalah gunaan fasilitas

	SNI-ISO 27001 A.8.2 Keamanan Sumber Daya Manusia (selama bekerja)	Memastikan bahwa semua pegawai, kontraktor, dan pengguna pihak ketiga telah peduli terhadap ancaman dan masalah keamanan informasi, tanggung jawab dan pertanggungan gugatan mereka dan disediakan perlengkapan yang memadai untuk mendukung kebijakan keamanan organisasi selama bekerja dan untuk mengurangi resiko kesalahan manusia
	SNI-ISO 27001 A.8.3 Keamanan Sumber Daya Manusia (pengakhiran atau perubahan pekerjaan)	Memastikan bahwa semua pegawai, kontraktor, dan pengguna pihak ketiga keluar dari organisasi atau adanya perubahan pekerjaan dengan cara yang sesuai
A.9	SNI-ISO 27001 A.9.1 Keamanan Fisik dan Lingkungan (*area* yang aman)	Mencegah akses fisik oleh pihak yang tidak berwenang, kerusakan dan interfensi terhadap lokasi dan informasi organisasi
	SNI-ISO 27001 A.9.2 Keamanan Fisik dan Lingkungan (keamanan peralatan)	Mencegah kehilangan, kerusakan, pencurian atau gangguan aset dan interupsi terhadap kegiatan organisasi
A.10	SNI-ISO 27001 A.10.1 Manajemen Komunikasi dan Operasi (prosedur operasional dan tanggung jawab)	Memastikan pengoperasian fasilitas pengolahan informasi secara benar dan aman

	SNI-ISO 27001 A.10.2 Manajemen Komunikasi dan Operasi (manajemen pelayanan jasa pihak ketiga)	Menerapkan dan memelihara tingkat keamanan informasi dan pelayanan jasa yang sesuai dengan perjanjian pelayanan jasa pihak ketiga
	SNI-ISO 27001 A.10.3 Manajemen Komunikasi dan Operasi (perencanaan dan ketertiban sistem)	Mengurangi resiko kegagalan sistem
	SNI-ISO 27001 A.10.4 Manajemen Komunikasi dan Operasi (perlindungan terhadap *malicious* dan *mobile code*)	Melindungi integritas perangkat lunak dan informasi
	SNI-ISO 27001 A.10.5 Manajemen Komunikasi dan Operasi (*backup*)	Memelihara integritas dan ketersediaan informasi dan fasilitas pengolahan informasi
	SNI-ISO 27001 A.10.6 Manajemen Komunikasi dan Operasi (manajemen keamanan jaringan)	Memastikan perlindungan informasi dalam jaringan dan perlindungan infrastruktur pendukung

	SNI-ISO 27001 A.10.7 Manajemen Komunikasi dan Operasi (penanganan *media*)	Mencegah pengungkapan, modifikasi, pemindahan atau pemusnahan aset yang tidak sah, dan gangguan kegiatan bisnis
	SNI-ISO 27001 A.10.8 Manajemen Komunikasi dan Operasi (pertukaran informasi)	Memelihara keamanan informasi dan perangkat lunak yang dipertukarkan dalam suatu organisasi dan dengan setiap entitas *eksternal*
	SNI-ISO 27001 A.10.9 Manajemen Komunikasi dan Operasi (layanan *electronic commers*)	Memastikan keamanan layanan *electronic commers* dan keamanan penggunanya
	SNI-ISO 27001 A.10.10 Manajemen Komunikasi dan Operasi (pemantauan)	Mendeteksi kegiatan pengolahan informasi yang tidak sah
A.11	SNI-ISO 27001 A.11.1 Pengendalian Akses (persyaratan bisnis untuk pengendalian akses)	Mengendalikan akses kepada informasi
	SNI-ISO 27001 A.11.2 Pengendalian Akses (manajemen akses pengguna)	Memastikan akses oleh pengguna yang sah dan untuk mencegah pihak yang tidak sah pada sistem informasi

	SNI-ISO 27001 A.11.3 Pengendalian Akses (tanggung jawab pengguna)	Mencegah akses pengguna yang tidak sah dan gangguan atau pencurian atas informasi dan fasilitas pengolahan informasi
	SNI-ISO 27001 A.11.4 Pengendalian Akses (jaringan)	Mencegah akses yang tidak sah kedalam layanan jaringan
	SNI-ISO 27001 A.11.5 Pengendalian Akses (sistem operasi)	Mencegah akses yang tidak sah kedalam layanan sistem operasi
	SNI-ISO 27001 A.11.6 Pengendalian Akses (aplikasi dan informasi)	Mencegah akses yang tidak sah terhadap informasi pada aplikasi sistem
	SNI-ISO 27001 A.11.7 Pengendalian Akses (*mobile computing* dan kerja jarak jauh/*teleworking*)	Memastikan keamanan informasi ketika menggunakan fasilitas *mobile computing* dan kerja jarak jauh (*teleworking*)
A.12	SNI-ISO 27001 A.12.1 Akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi (persyaratan keamanan dari sistem informasi)	Memastikan bahwa keamanan merupakan bagian utuh dari sistem informasi

	SNI-ISO 27001 A.12.2 Akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi (pengolahan yang benar dalam aplikasi)	Mencegah kesalahan, kehilangan, modifikasi yang tidak sah atau penyalahgunaan informasi dalam aplikasi
	SNI-ISO 27001 A.12.3 Akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi (pengendalian dengan cara kriptografi)	Melindungi kerahasiaan, keaslian, atau integritas informasi dengan cara kriptografi
	SNI-ISO 27001 A.12.4 Akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi (keamanan *system files*)	Memastikan keamanan *system files*
	SNI-ISO 27001 A.12.5 Akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi (keamanan dalam proses pengembangan dan pendukung)	Memelihara keamanan perangkat lunak sistem aplikasi dan informasi
	SNI-ISO 27001 A.12.6 Akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi (manajemen kerawanan teknis)	Mengurangi resiko terhadap eksploitasi kerawanan teknis yang dipublikasikan

A.13	SNI-ISO 27001 A.13.1 Manajemen Insiden Keamanan Informasi (pelaporan kejadian dan kelemahan keamanan informasi)	Memastikan kejadian dan kelemahan keamanan informasi terkait dengan sistem informasi dikomunikasikan sedemikian rupa sehingga memungkinkan tindakan koreksi dapat dilakukan tepat waktu
	SNI-ISO 27001 A.13.2 Manajemen Insiden Keamanan Informasi (perbaikan)	Memastikan pendekatan yang konsisten dan efektif diterapkan untuk manajemen insiden keamanan informasi
A.14	SNI-ISO 27001 A.14.1 Manajemen Keberlanjutan Bisnis (aspek keamanan informasi)	Menghadapi gangguan kegiatan bisnis dan untuk melindungi proses bisnis kritis dari efek kegagalan utama sistem informasi atau bencana dan untuk memastikan keberlanjutannya secara tepat waktu
A.15	SNI-ISO 27001 A.15.1 Kesesuaian (persyaratan hukum)	Mencegah pelanggaran terhadap undang-undang, peraturan perundang-undangan, atau kewajiban kontrak dan setian persyaratan keamanan
	SNI-ISO 27001 A.15.2 Kesesuaian (pemenuhan terhadap kebijakan keamanan standar, pemenuhan teknis)	Memastikan pemenuhan sistem terhadap kebijakan dan standar keamanan organisasi
	SNI-ISO 27001 A.15.3 Kesesuaian (pertimbangan audit sistem informasi)	Memaksimalkan keefektifan dari dan untuk meminimalkan interfensi kepada/dari proses audit sistem informasi

LAMPIRAN 2

Tabel Hasil Dari *Scanning* Ip Dengan Zenmap Pada Jaringan Laptop Kali Linux

No	*Address*	*Port*	*State*	*Service*	*Version*
1	10.20.208.1	22/tcp	*Open*	Ssh	AllegroSoft RomSShell sshd 5.40 (*protocol* 2.0)
		443/tcp	*Open*	http	AllegroSoft RomPager 5.40
2	10.60.52.1	22/tcp	*Open*	Ssh	AllegroSoft RomSShell sshd 5.40 (*protocol* 2.0)
		161/tcp	*Filtered*	Snmp	tidak ditemukan
		443/tcp	*Open*	http	AllegroSoft RomPager 5.40
3	10.60.52.2	23/tcp	*Open*	telnet	tidak ditemukan
		80/tcp	*Open*	http	ZK *Web Server* (ZK*Software* ZEM500 *fingerprint reader*; MIPS)

4	10.60.52.3	80/tcp	*Open*	http	Apache httpd 2.2.14((Win32) DAV/mod_ssl/2.2.14 OpenSSL/0.9.8I mod_*autoindex*_color PHP/5.3.1 mod_apreq2-2009110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)
		135/tcp	*Open*	Msrpc	Microsoft Windows RPC
		139/tcp	*Open*	Netbios-ssn	Microsoft Windows netbios-ssn
		445/tcp	*Open*	Microsoft-ds	tidak ditemukan
		49152 /tcp	*Open*	Msrpc	Microsoft Windows RPC
		49153 /tcp	*Open*	Msrpc	Microsoft Windows RPC
		49154 /tcp	*Open*	Msrpc	Microsoft Windows RPC
		49155 /tcp	*Open*	Msrpc	Microsoft Windows RPC
5	10.60.52.184	135/tcp	*Open*	Msrpc	Microsoft Windows RPC
		139/tcp	*Open*	Netbios-ssn	Microsoft Windows netbios-ssn
		445/tcp	*Open*	Microsoft-ds	tidak ditemukan
		2869/tcp	*Open*	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
		49156 /tcp	*Open*	Msrpc	Microsoft Windows RPC

6	10.60.52.185	135/tcp	*Open*	Msrpc	Microsoft Windows RPC
		139/tcp	*Open*	Netbios-ssn	Microsoft Windows netbios-ssn
		445/tcp	*Open*	Microsoft-ds	tidak ditemukan
		49152 /tcp	*Open*	Msrpc	Microsoft Windows RPC
		49153 /tcp	*Open*	Msrpc	Microsoft Windows RPC
		49154 /tcp	*Open*	Msrpc	Microsoft Windows RPC
		49155 /tcp	*Open*	Msrpc	Microsoft Windows RPC
		49156 /tcp	*Open*	Msrpc	Microsoft Windows RPC
		49160 /tcp	*Open*	Msrpc	Microsoft Windows RPC
		49163 /tcp	*Open*	Msrpc	Microsoft Windows RPC
7	10.60.52.186	135/tcp	*Open*	Msrpc	Microsoft Windows RPC
		139/tcp	*Open*	Netbios-ssn	Microsoft Windows netbios-ssn
		445/tcp	*Open*	Microsoft-ds	Windows 7 Home Basic 7601 *Service Pack* 1 microsoft-ds (workgroup: WORKGROUP)
		49156 /tcp	*Open*	Msrpc	Microsoft Windows RPC

8	10.60.52.188	135/tcp	*Open*	Msrpc	Microsoft Windows RPC
		139/tcp	*Open*	Netbios-ssn	Microsoft Windows netbios-ssn
		445/tcp	*Open*	Microsoft-ds	Windows 7 Home Basic 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
		5357 /tcp	*Open*	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9	10.60.52.190	135/tcp	*Open*	Msrpc	Microsoft Windows RPC
		139/tcp	*Open*	Netbios-ssn	Microsoft Windows netbios-ssn
		445/tcp	*Open*	Microsoft-ds	tidak ditemukan

10	10.60.52.191	135/tcp	*Open*	Msrpc	Microsoft Windows RPC
		139/tcp	*Open*	Netbios-ssn	Microsoft Windows netbios-ssn
		445/tcp	*Open*	Microsoft-ds	Windows 7 Home Basic 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
		49152 /tcp	*Open*	Msrpc	Microsoft Windows RPC
		49153 /tcp	*Open*	Msrpc	Microsoft Windows RPC
		49154 /tcp	*Open*	Msrpc	Microsoft Windows RPC
		49155 /tcp	*Open*	Msrpc	Microsoft Windows RPC
		49156 /tcp	*Open*	Msrpc	Microsoft Windows RPC
		49159 /tcp	*Open*	Msrpc	Microsoft Windows RPC
11	10.60.52.192	tidak ditemukan	tidak ditemukan	tidak ditemukan	tidak ditemukan
12	10.60.52.225	tidak ditemukan	tidak ditemukan	tidak ditemukan	tidak ditemukan
13	10.60.52.233	6646 /tcp	*Open*	*tcpwrapped*	tidak ditemukan

LAMPIRAN 3

Audit *Charter*

Audit Charter

Project ID : ISO 27001 – Audit

Project Name : Audit Keamanan Sistem Informasi

Auditor : Ferdian Noor Pambudi

Project Description :

Penelitian yang berkaitan dengan keamanan informasi ini menggunakan parameter ISO 27001. Penelitian ini berfokus pada klausul kebijakan keamanan, pengelolaan aset, keamanan fisik dan lingkungan, manajemen komunikasi dan operasi, serta pengendalian akses.

Project Schedule :

Stakeholder list :

Jabatan	Responden	Klausul Pengendalian
Sarana dan Prasarana	Alfian	Kebijakan keamanan, ISO 27001 A.5 (A.5.1)
Operator SIMAK BMN	Nuromah	Pengelolaan aset, ISO 27001 A.7 (A.7.1 – A.7.2)
Perawat	Ari Rahmadi	Keamanan fisik dan lingkungan, ISO 27001 A.9 (A.9.1 – A.9.2)
Administrasi	Farhanati M.	Manajemen komunikasi dan operasi, ISO 27001 A.10 (A.10.1 – A.10.5 – A.10.6)
Bagian Keuangan	Ulfah	Pengendalian akses, ISO 27001 A.11 (A.11.5)

Yogyakarta, 7 Agustus 2019

Mengetahui

Kepala Klinik Pratama UIN Yogyakarta	Auditor
Dr. Diana Rismajani	Ferdian Noor Pambudi
NIP : 19710729 200502 2 003	NIM : 12650025

LEMBAR KERTAS KERJA AUDIT

Analisis Keamanan Sistem Informasi dan Administrasi

Klinik Pratama UIN Yogyakarta

Standar ISO 27001

Document ID	: INTERVIEW – 01
Project Name	: Audit Keamanan Sistem Informasi
Auditor	: Ferdian Noor Pambudi
Audite	: Alfian
Description	: Lembar kertas kerja audit ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar kertas kerja audit ini digunakan untuk mengevaluasi Kebijakan Keamanan yang diterapkan oleh pengelola Sistem Informasi dan Administrasi Klinik Pratama UIN Yogyakarta
Date	: 7 Agustus 2019
Responsible	: Sarana dan Prasarana

Approved by

Alfian

Auditor

Ferdian Noor Pambudi

LEMBAR KERTAS KERJA AUDIT

Analisis Keamanan Sistem Informasi dan Administrasi

Klinik Pratama UIN Yogyakarta

Standar ISO 27001

Document ID	:	INTERVIEW – 02
Project Name	:	Audit Keamanan Sistem Informasi
Auditor	:	Ferdian Noor Pambudi
Audite	:	Nuromah
Description	:	Lembar kertas kerja audit ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta Lembar kertas kerja audit ini digunakan untuk mengevaluasi Pengelolaan Aset yang diterapkan oleh pengelola Sistem Informasi dan Administrasi Klinik Pratama UIN Yogyakarta
Date	:	
Responsible	:	Operator SIMAK BMN

Approved by

Nuromah

Auditor

Ferdian Noor Pambudi

LEMBAR KERTAS KERJA AUDIT

Analisis Keamanan Sistem Informasi dan Administrasi

Klinik Pratama UIN Yogyakarta

Standar ISO 27001

Document ID	:	INTERVIEW – 03
Project Name	:	Audit Keamanan Sistem Informasi
Auditor	:	Ferdian Noor Pambudi
Audite	:	Ari Rahmadi
Description	:	Lembar kertas kerja audit ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar kertas kerja audit ini digunakan untuk mengevaluasi Keamanan Fisik dan Lingkungan yang diterapkan oleh pengelola Sistem Informasi dan Administrasi Klinik Pratama UIN Yogyakarta
Date	:	
Responsible	:	Perawat

Approved by

Ari Rahmadi

Auditor

Ferdian Noor Pambudi

LEMBAR KERTAS KERJA AUDIT

Analisis Keamanan Sistem Informasi dan Administrasi

Klinik Pratama UIN Yogyakarta

Standar ISO 27001

Document ID	:	INTERVIEW – 04
Project Name	:	Audit Keamanan Sistem Informasi
Auditor	:	Ferdian Noor Pambudi
Audite	:	Farhanati M.
Description	:	Lembar kertas kerja audit ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta Lembar kertas kerja audit ini digunakan untuk mengevaluasi Manajemen Komunikasi dan Operasi yang diterapkan oleh pengelola Sistem Informasi dan Administrasi Klinik Pratama UIN Yogyakarta
Date	:	
Responsible	:	Administrasi

Approved by

Farhanati M.

Auditor

Ferdian Noor Pambudi

LEMBAR KERTAS KERJA AUDIT

Analisis Keamanan Sistem Informasi dan Administrasi

Klinik Pratama UIN Yogyakarta

Standar ISO 27001

Document ID	:	INTERVIEW – 05
Project Name	:	Audit Keamanan Sistem Informasi
Auditor	:	Ferdian Noor Pambudi
Audite	:	Ulfah
Description	:	Lembar kertas kerja audit ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta Lembar kertas kerja audit ini digunakan untuk mengevaluasi Pengendalian Akses yang diterapkan oleh pengelola Sistem Informasi dan Administasi Klinik Pratama UIN Yogyakarta
Date	:	
Responsible	:	Bagian Keuangan

Approved by

Ulfah

Auditor

Ferdian Noor Pambudi

LAMPIRAN 4

LEMBAR KUISIONER

QUESTIONS OF INTERVIEW

Document ID : INTERVIEW - 01
Klausul : Kebijakan Keamanan (A.5)

No	Code	Question	Answer	Score
1	Q1	Sudah adakah kebijakan keamanan informasi?	Sudah, direncanakan	2
2	Q2	Apakah kebijakan keamanan tersebut sudah didokumentasikan?	belum	1
3	Q3	Apabila sudah, apakah dokumen kebijakan keamanan informasi itu sudah disetujui oleh pihak manajemen?	belum	1
4	Q4	Apakah dokumen kebijakan tersebut sudah di publikasikan kepada semua pihak terkait?	belum	1
5	Q5	Apakah kebijakan tersebut sudah dikomunikasikan?	belum	1
6	Q6	Apakah sudah dilakukan tinjauan ulang terhadap kebijakan keamanan informasi (untuk antisipasi perubahan yang mempengaruhi analisa resiko)?	belum	1
7	Q7	Apakah tinjauan ulang kebijakan dilakukan secara berkala dan terjadwal?	belum	0
8	Q8	Apabila terjadi perubahan mengenai kebijakan, apakah kebijakan tersebut merupakan pengembangan dari sebelumnya (guna memenuhi kebutuhan dan efektif dalam pelaksanaan)?	belum	0
9	Q9	Apakah kebijakan yang diterapkan sudah sesuai dengan aturan yang berlaku?	belum	1
10	Q10	Siapakah yang bertanggung jawab terhadap kebijakan keamanan informasi?	Bu Farhan dan ba Westri	4

QUESTIONS OF INTERVIEW

Document ID : INTERVIEW - 02
Klausul : Pengelolaan Aset (A.7)

No	Code	Question	Answer	Score
1	Q11	Apakah semua inventaris aset (informasi, perangkat lunak, fisik dan layanan) sudah diidentifikasi dan dicatat?	Ada	4
2	Q12	Apakah inventaris aset tersebut dijaga dan dipelihara?	Ada, di setiap unit pelayanan	4
3	Q13	Apakah sudah diterapkan kebijakan pengelolaan aset?	Sudah	3
4	Q14	Apakah kebijakan pengelolaan inventaris aset tersebuh sudah didokumentasikan?	sudah	3
5	Q15	Apakah ada pegawai / petugas yang menjaga (mengontrol dan memelihara) keamanan informasi inventaris aset?	sudah	2
6	Q16	Siapa yang bertanggung jawab mengontrol dan memelihara terhadap pemrosesan informasi tersebut?	Bu Nurohmah	4
7	Q17	Apakah ada jangka waktu pengecekan inventaris aset secara berkala?	ada, seminggu sekali	2
8	Q18	Apakah sudah diidentifikasi nilai dan tingkat kepentingan aset?	sudah	4
9	Q19	Apakah terdapat aturan dalam menggunakan informasi yang berhubungan dengan fasilitas pemrosesan informasi (misal hardware server)?	Belum	0
10	Q20	Apakah aturan dalam menggunakan aset informasi tersebut sudah di implementasikan?	Sudah	5

11	Q21	Adakah dokumentasi mengenai informasi pengelolaan aset?	Ada	3
12	Q22	Apakah informasi aset sudah diklasifikasikan dengan tingkat perlindungan yang tepat?	Ada	4
13	Q23	Apakah ada prosedur yang baik berupa pemberi tanda pelabelan dan penanganan informasi?	Ada	3
14	Q24	Apakah prosedur pelabelan dan penanganan informasi harus sesuai dengan skema klasifikasi informasi?	Ada	3

QUESTIONS OF INTERVIEW

Document ID : INTERVIEW - 03
Klausul : Keamanan Fisik dan Lingkungan (A.9)

No	Code	Question	Answer	Score
1	Q25	Apakah terdapat petugas yang berjaga dipintu masuk, guna meminimalisir resiko pencurian atau kesalahan dalam penggunaan fasilitas?	Belum	0
2	Q26	Apakah terdapat aturan tertentu ketika memasuki ruang pemrosesan informasi?	Belum	1
3	Q27	Apakah ada kontrol akses fisik atau ruang / wilayah sebagai tempat menerima tamu?	Ada	2
4	Q28	Pernahkah meninggalkan komputer dalam keadaan menyala dan ada pegawai lain di dalamnya?	Pernah	2
5	Q29	Adakah ruangan khusus atau pembatas seperti dinding bagi pemegang kendali sistem informasi kearsipan statis?	Belum, sebagian sudah (Keuangan, Data kepegawaian, Rekam medis)	2
6	Q30	Apakah tembok terluar bangunan sudah terbuat dari konstruksi kuat dan terlindung dari akses tanpa izin?	Belum	1
7	Q31	Apakah pengunjung yang datang diawasi dan menulis tanggal datang dibuku tamu?	Belum	0
8	Q32	Apakah hak akses ke ruang informasi dan fasilitas pemrosesan informasi selalu dikontrol dan dibatasi?	Ada	2
9	Q33	Apakah semua pegawai dan karyawan diwajibkan memakai tanda pengenal?	~~Belum~~ ~~Atau~~ Belum	1
10	Q34	Apakah sudah diidentifikasi siapa saja yang berhak masuk ruangan kantor, guna memastikan keamanan kantor tetap terjaga?	Sudah	2

11	Q35	Apakah sudah ada perlindungan fisik terhadap kerusakan akibat dari ledakan, banjir dan bencana alam lainnya?	Ada	4
12	Q36	Apakah bahan yang berbahaya dan mudah meledak sudah disimpan diwilayah aman?	Sudah	3
13	Q37	Apakah penempatan ruang sistem informasi / server sudah termasuk dalam area yang aman?	Sudah	3
14	Q38	Apakah terdapat kebijakan mengenai makan, minum dan merokok disekitar fasilitas pemrosesan informasi?	Ada	3
15	Q39	Apakah kabel listrik sudah dipisahkan dari kabel komunikasi untuk mencegah gangguan (interferensi)?	Sudah	3
16	Q40	Apakah komputer server dan peralatan informasi sudah dicek dan ditempatkan pada tempat yang aman?	Sudah	2
17	Q41	Apakah tata letak hardware sudah ditempatkan dengan tepat guna memastikan tidak ada peluang akses oleh pihak yang tidak berwenang?	Sudah	2
18	Q42	Apakah peralatan sudah dilindungi dari kegagalan daya listrik?	Sudah	3
19	Q43	Apakah sudah tersedia peralatan pendukung cadangan seperti genset atau UPS?	Belum	1
20	Q44	Apakah utilitas pendukung seperti sumber daya listrik, genset, UPS selalu dicek keamanannya?	Belum	1
21	Q45	Apakah kabel daya dan telekomunikaasi kebutuhan data sudah dilindungi dari ancaman kerusakan atau penyadapan misal pencurian listrik / menggunakan pipa pengaman?	~~Sebagian~~ Belum	1
22	Q46	Apakah peralatan Hardware selalu dijaga dan dipelihara dengan baik?	Iya	4

23	Q47	Apakah ada prosedur dalam menggunakan peralatan / hardware?	Ada	3
24	Q48	Apakah waktu pengecekan peralatan / hardware sudah sesuai dengan prosedur yang ada?	sudah	2

QUESTIONS OF INTERVIEW

Document ID : INTERVIEW - 04
Klausul : Manajemen Komunikasi dan Operasi (A.10)

No	Code	Question	Answer	Score
1	Q49	Apakah terdapat prosedur pengoperasian dalam pemrosesan informasi (guna memastikan keamanan operasi)?	Ada, Sesuai dengan Tugas pokok dan Fungsi karyawan	3
2	Q50	Jika ada, apakah prosedur sudah di dokumentasikan dan tersedia bagi pengguna?	Belum	1
3	Q51	Apakah pengoperasian fasilitas pengolahan informasi (Maintenance Server) sudah dilakukan secara benar dan aman?	Sudah	2
4	Q52	Apakah setiap data penting dilakukan back-up?	Iya	3
5	Q53	Jika ada perubahan terhadap fasilitas dan sistem pengolahan informasi, apakah akan dikomunikasikan kepada pihak terkait?	Iya	3
6	Q54	Apakah pegawai di ruang sistem informasi sudah dipisahkan menujrut tugas dan tanggung jawabnya masing-masing?	Sudah	3
7	Q55	Apakah ada pengawasan dan pemantauan terhadap sistem untuk mengurangi resiko / insiden penyalahgunaan atau modifikasi tanpa ijin?	Ada	2
8	Q56	Apakah perangkat lunak / software dilakukan uji secara berkala?	Iya	3
9	Q57	Apakah setiap data berupa informasi dilakukan back-up guna mencegah terjadinya kehilangan atau kegagalan?	Iya	3

10	Q58	Apakah salinan back-up dan prosedur pemulihan yang terdokumentasi disimpan di lokasi terpisah?	Iya	3
11	Q59	Apakah media back-up tersebut sudah diuji secara berkala untuk memastikan bisa digunakan pada situasi darurat?	Sudah	3
12	Q60	Apakah sudah menerapkan kontrol jaringan untuk memastikan keamanan sistem dan data dalam jaringan?	Sudah	3
13	Q61	Apakah kontrol tersebut dilakukan secara berkala, guna melindungi hak akses tanpa ijin pada jaringan / serangan?	Iya	3
14	Q62	Sejauh ini, apahak terdapat titik jaringan yang rawan terhadap serangan?	Ada, Ruang rekam medis	2
15	Q63	Apakah ada petugas atau pegawai yang khusus menangani keamanan jaringan?	Ga ada	0
16	Q64	Apakah sudah terdapat mekanisme pengamanan jaringan sebagai upaya pencegahan serangan?	Belum	0
17	Q65	Apabila serangan telah terjadi, adakah mekanisme recovery jaringan yang diterapkan?	Belum	0

QUESTIONS OF INTERVIEW

Document ID : INTERVIEW - 05
Klausul : Pengendalian Akses (A.11)

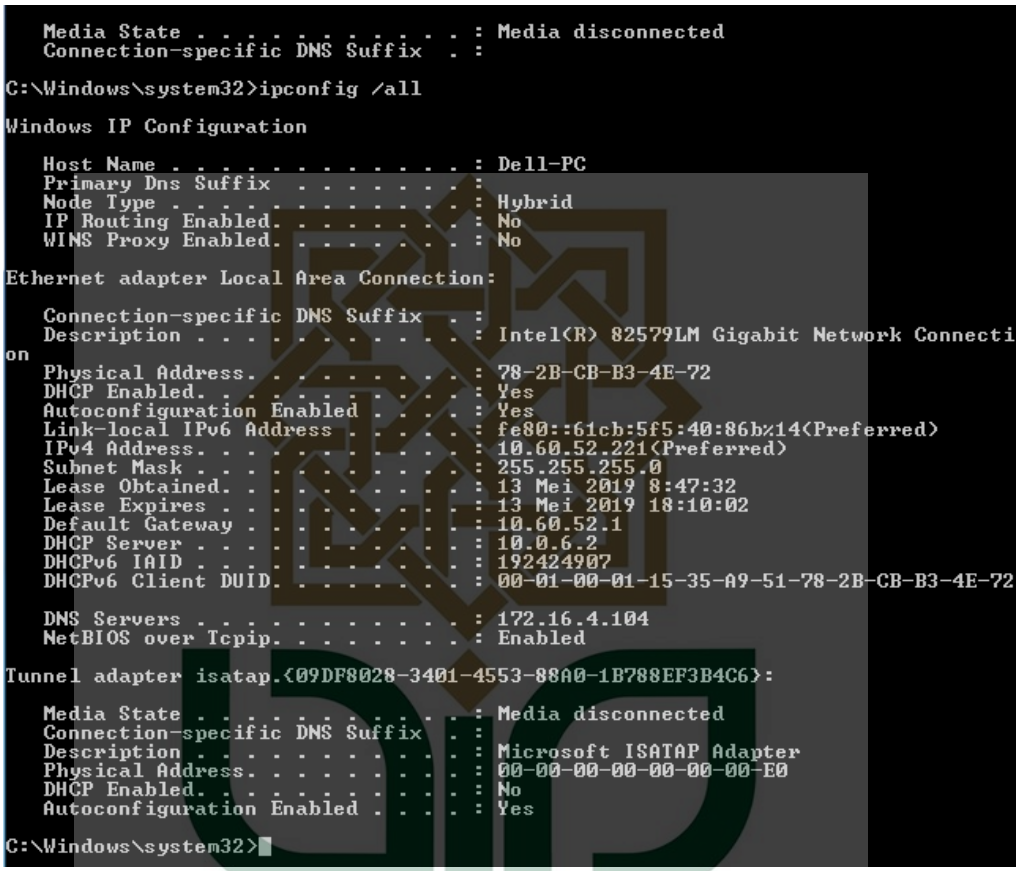
No	Code	Question	Answer	Score
1	Q66	Apakah sudah diterapkan prosedur log-in pada sistem informasi?	Sudah	5
2	Q67	Apakah sistem sudah membatasi kegagalan percobaan log-in?	Sudah	3
3	Q68	Apakah seluruh pengguna (termasuk staf pendukung teknis) memiliki user ID yang berbeda?	Iya	5
4	Q69	Apakah user ID tersebut disyaratkan agar mempunyai ID yang unik seperti menggabungkan huruf dan angka?	Sudah	4
5	Q70	Apakah sudah ada sistem manajemen password dan sistem pengelolaan password untuk memastikan kualitas password?	bisa	3
6	Q71	Apakah terdapat prosedur batasan jangka waktu pemakaian akun user?	belum	1
7	Q72	Sudah adakah prosedur penonaktifan akun user (seperti password) guna memastikan tidak adanya pemakaian ulang?	bisa	5
8	Q73	Apakah sudah menggunakan sesi time-out?	belum	1

LAMPIRAN

PENETRATION TESTING

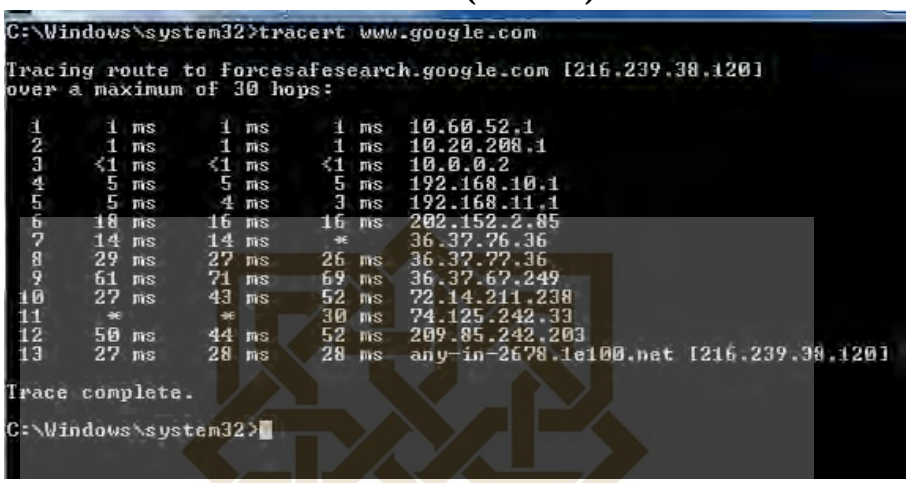
LAMPIRAN 5

Tampilan Hasil Dengan Ipconfig Pada Komputer Pegawai Sarana dan Prasarana (Dell-PC)



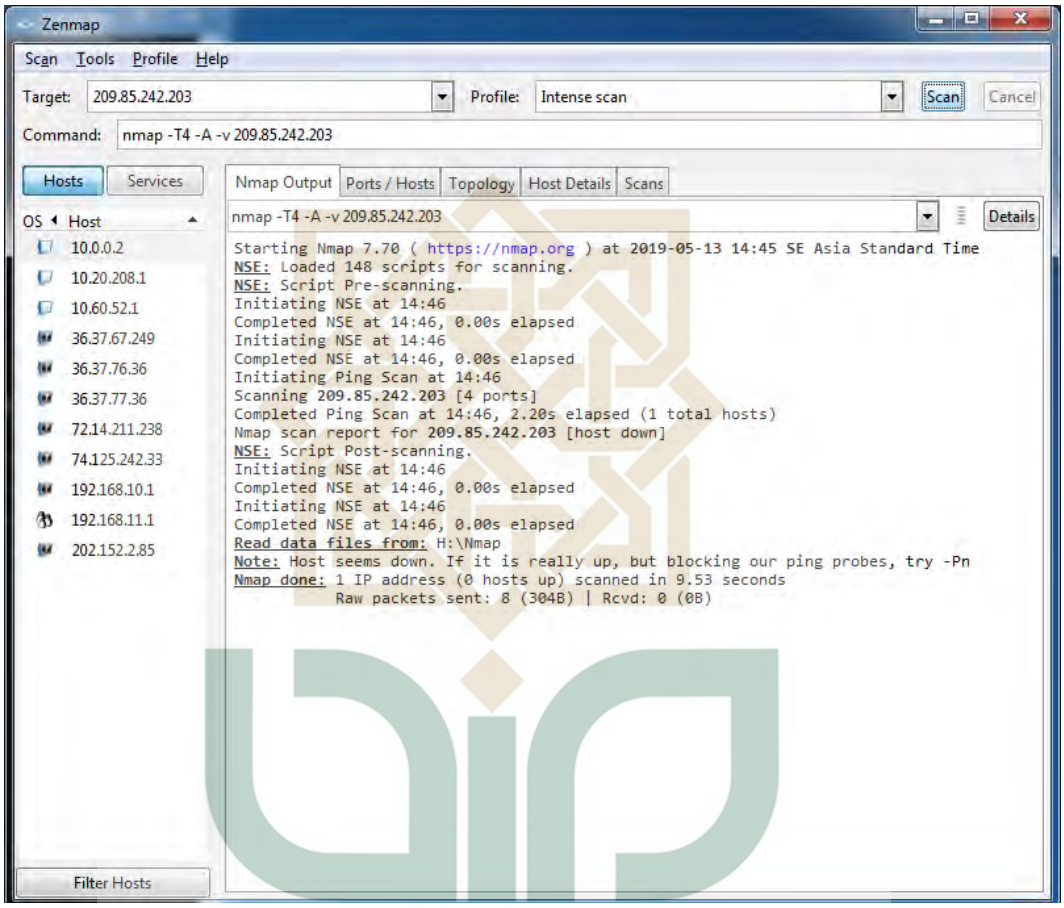
LAMPIRAN 6

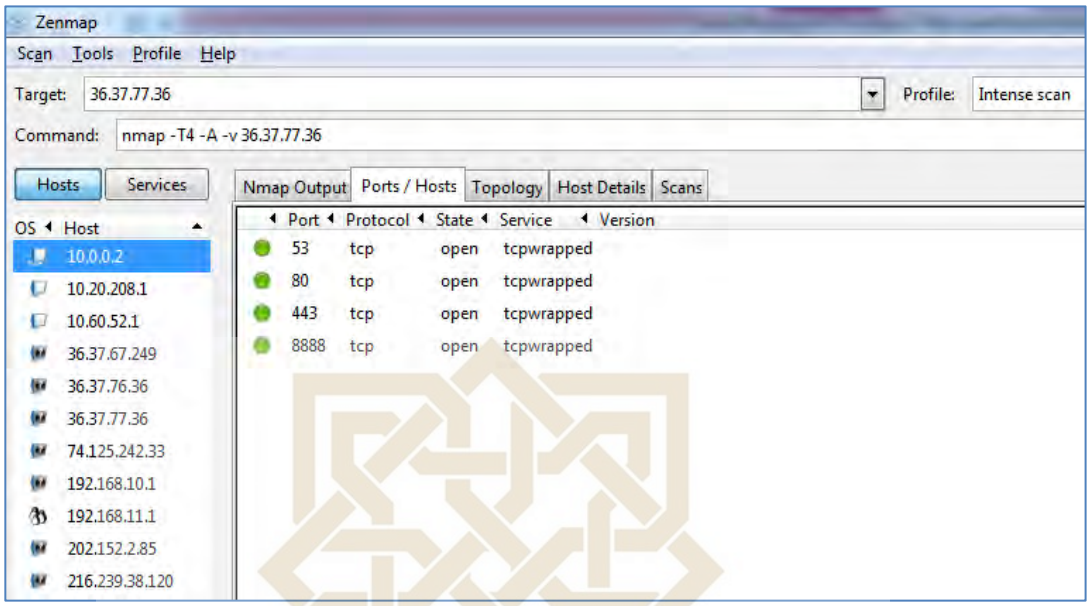
Tampilan Hasil Dengan Traceroute Pada Komputer Pegawai Sarana dan Prasarana (Dell-PC)

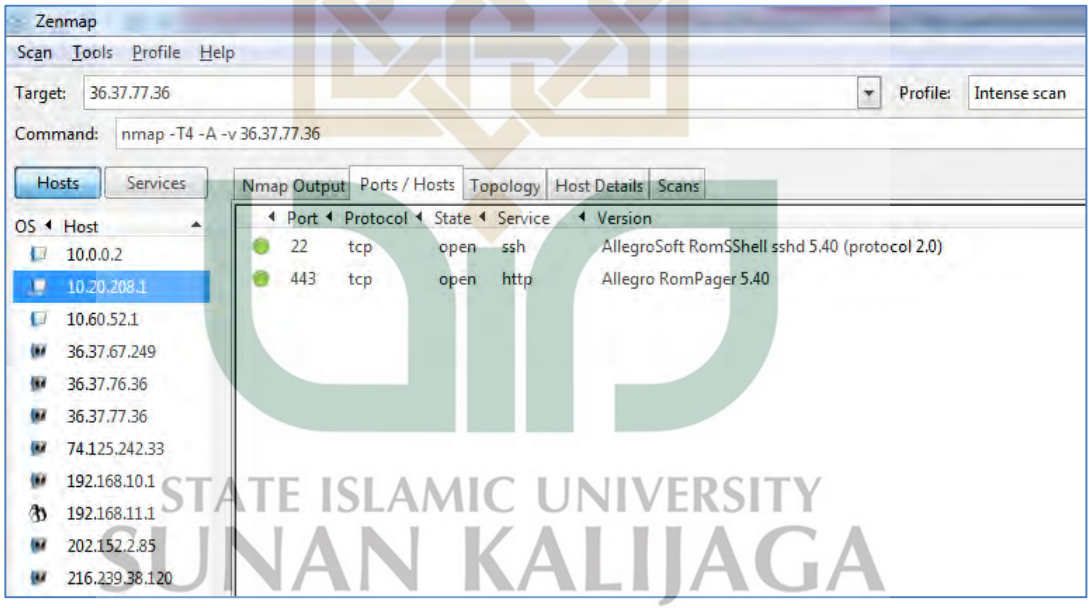


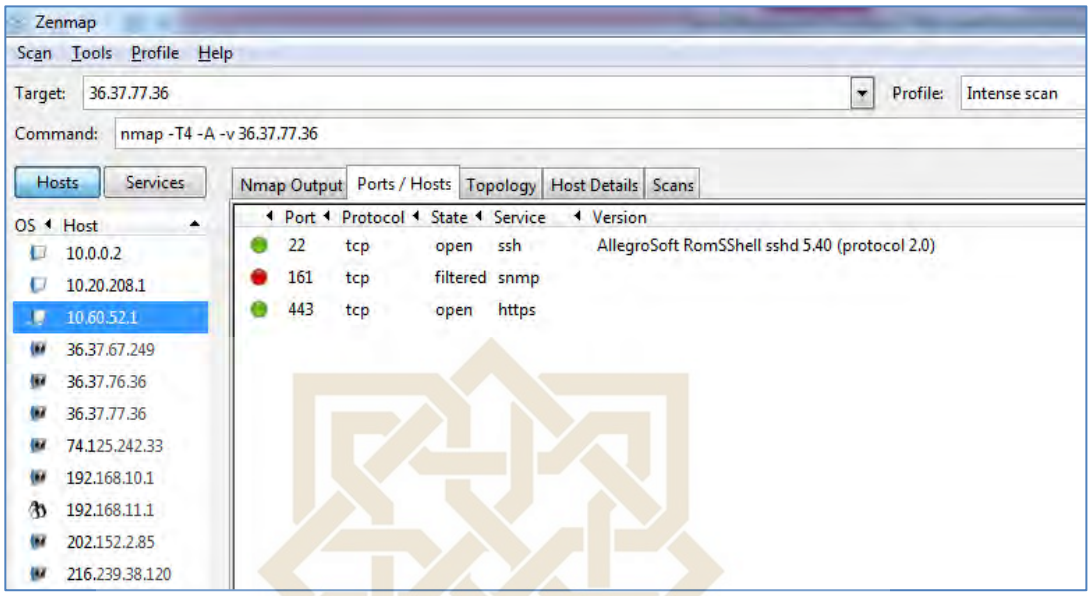
LAMPIRAN 7

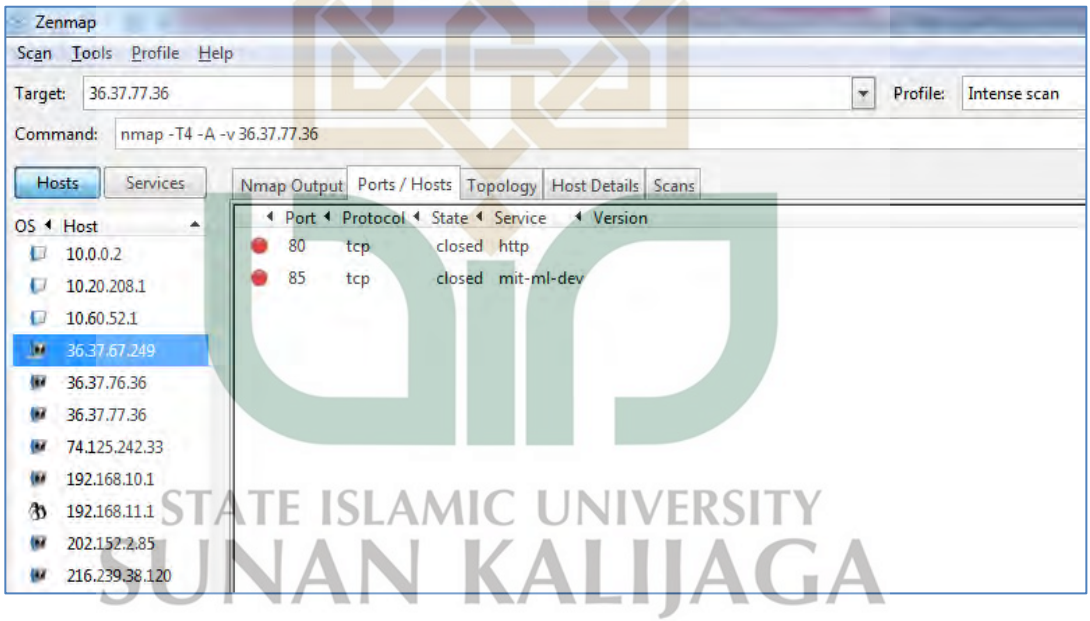
Tampilan Hasil Ip *Scanning* Dengan Zenmap Pada Komputer Pegawai Sarana dan Prasarana (Dell-PC)

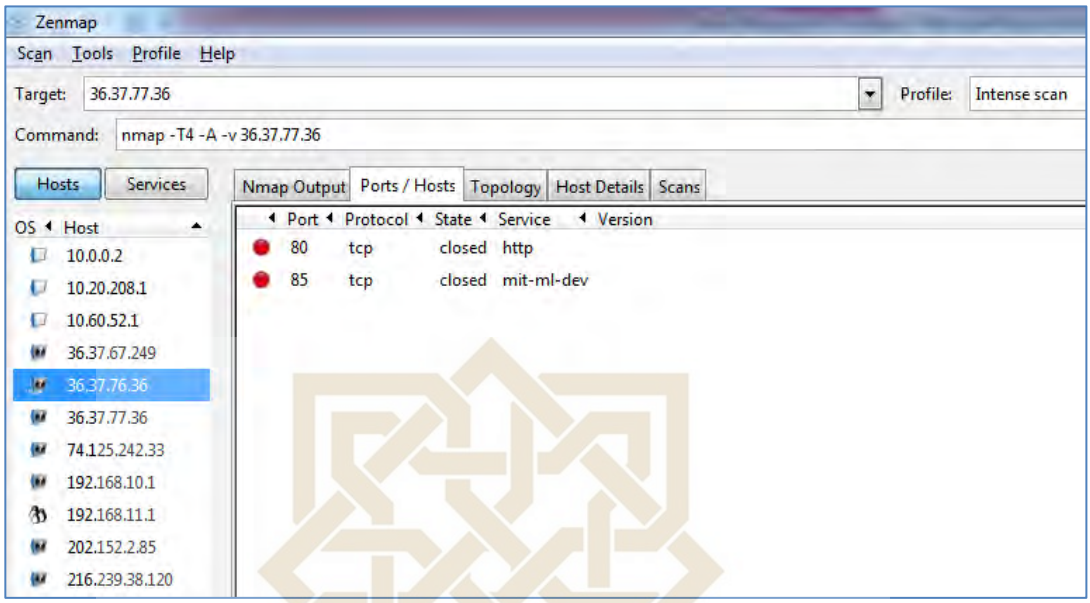


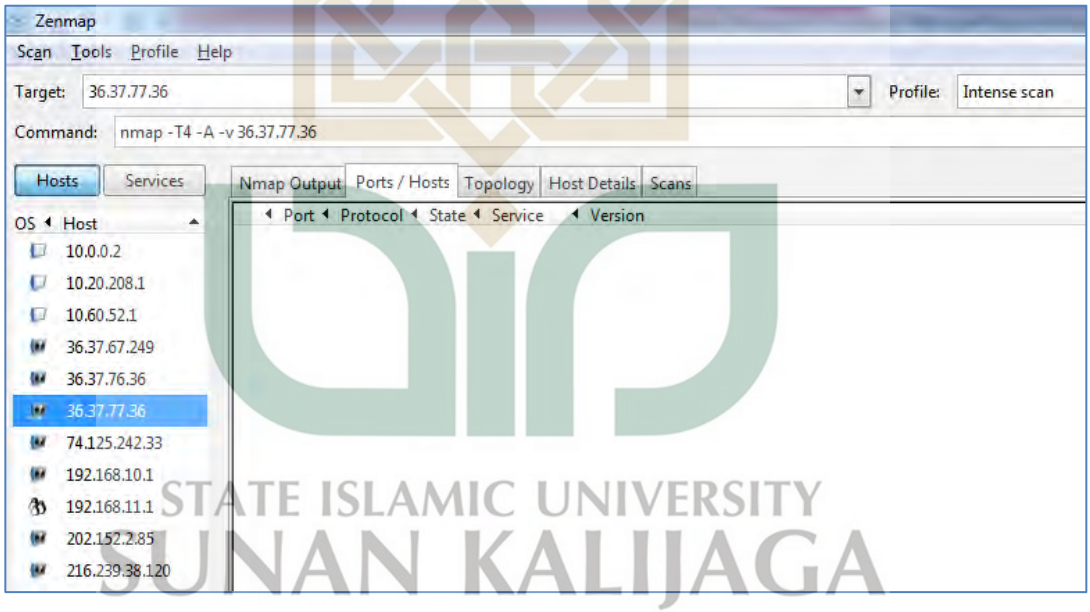


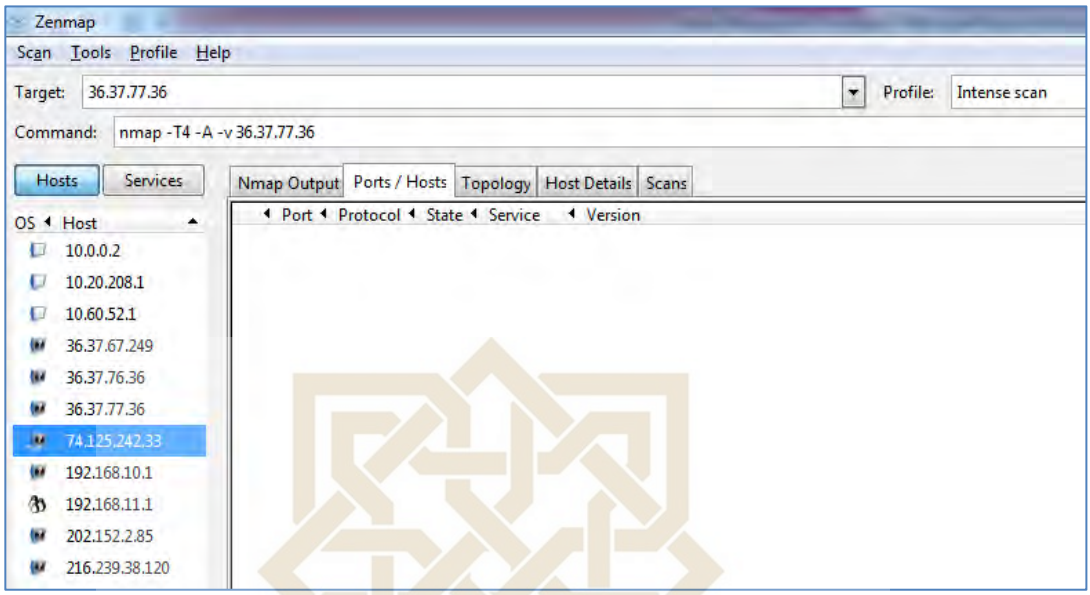


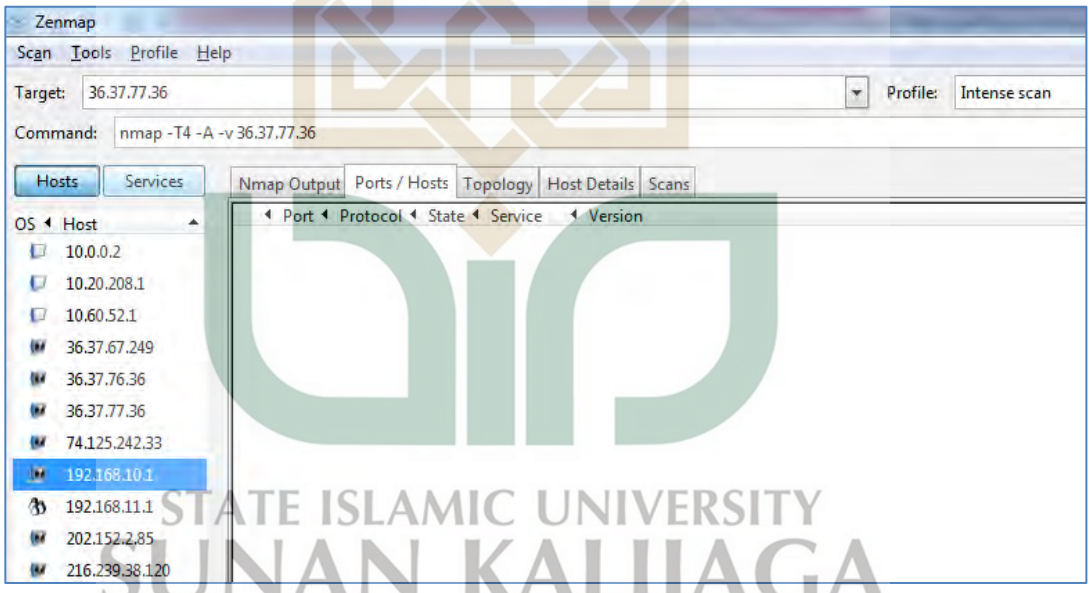


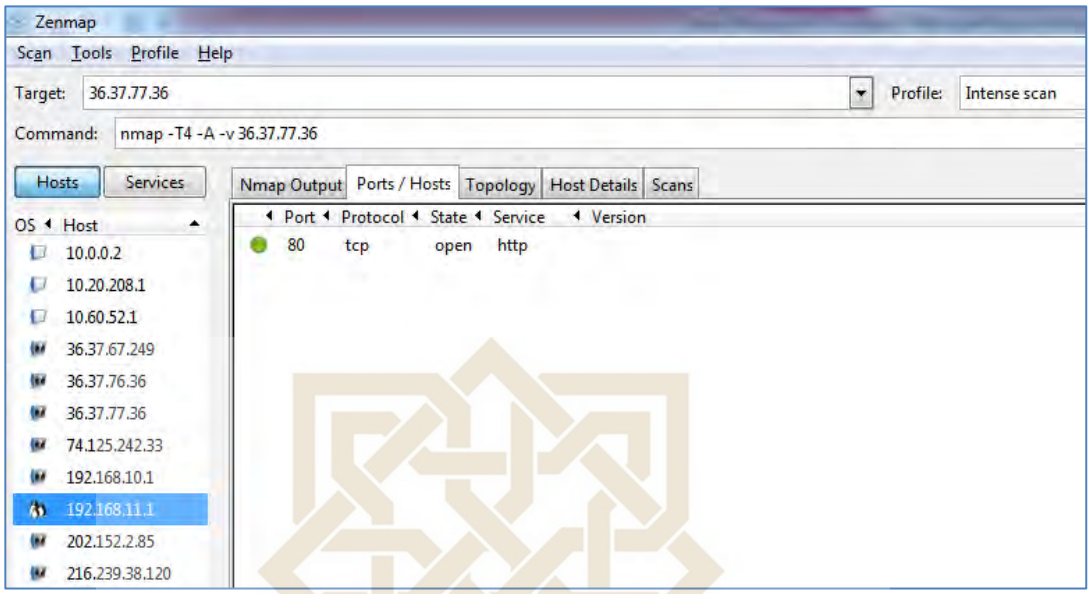


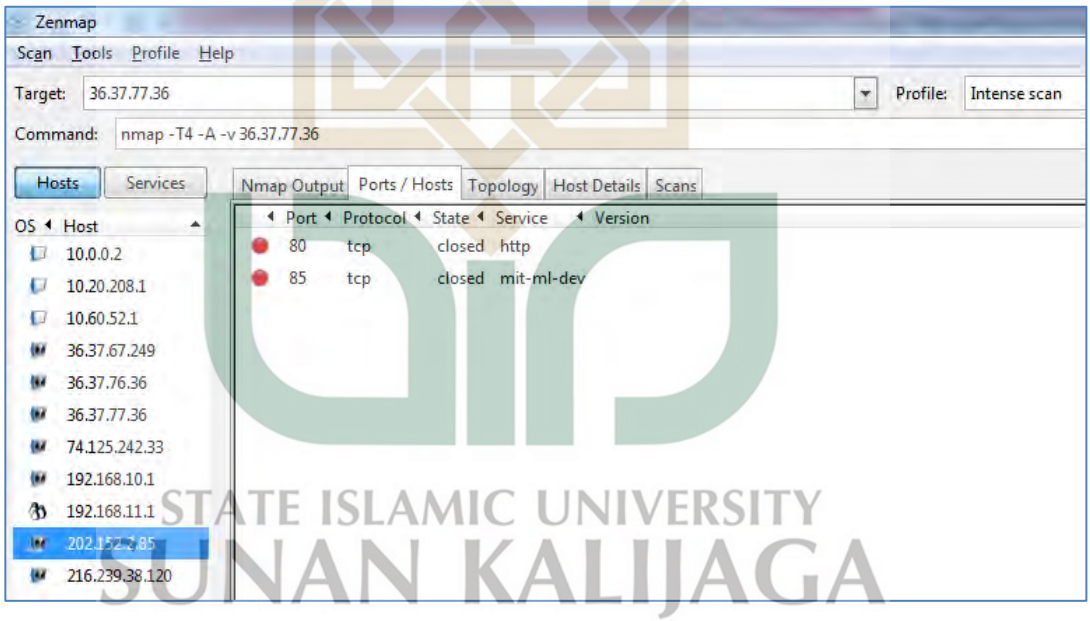


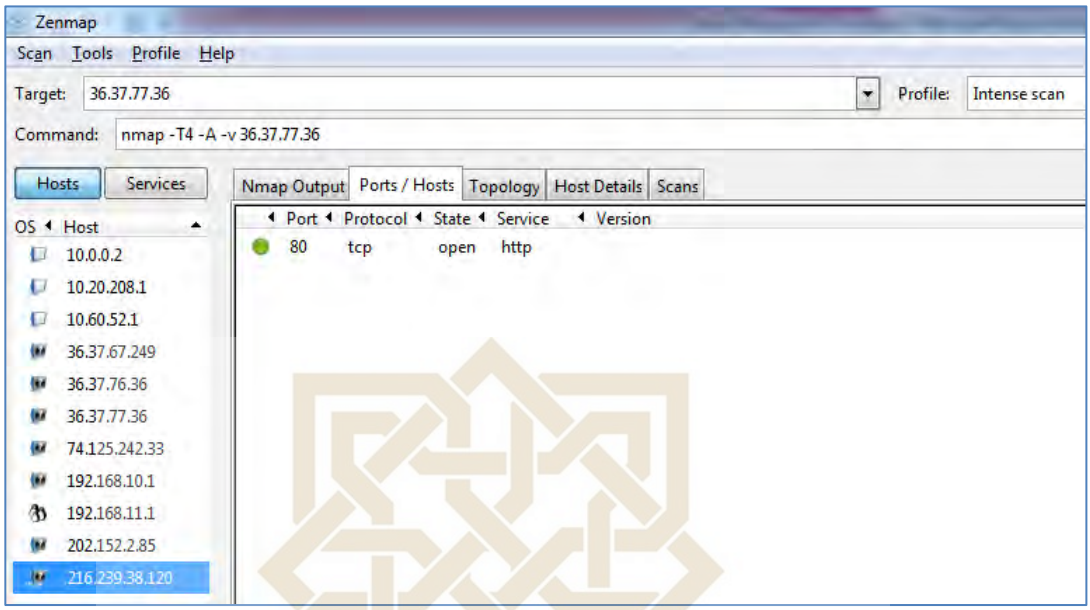






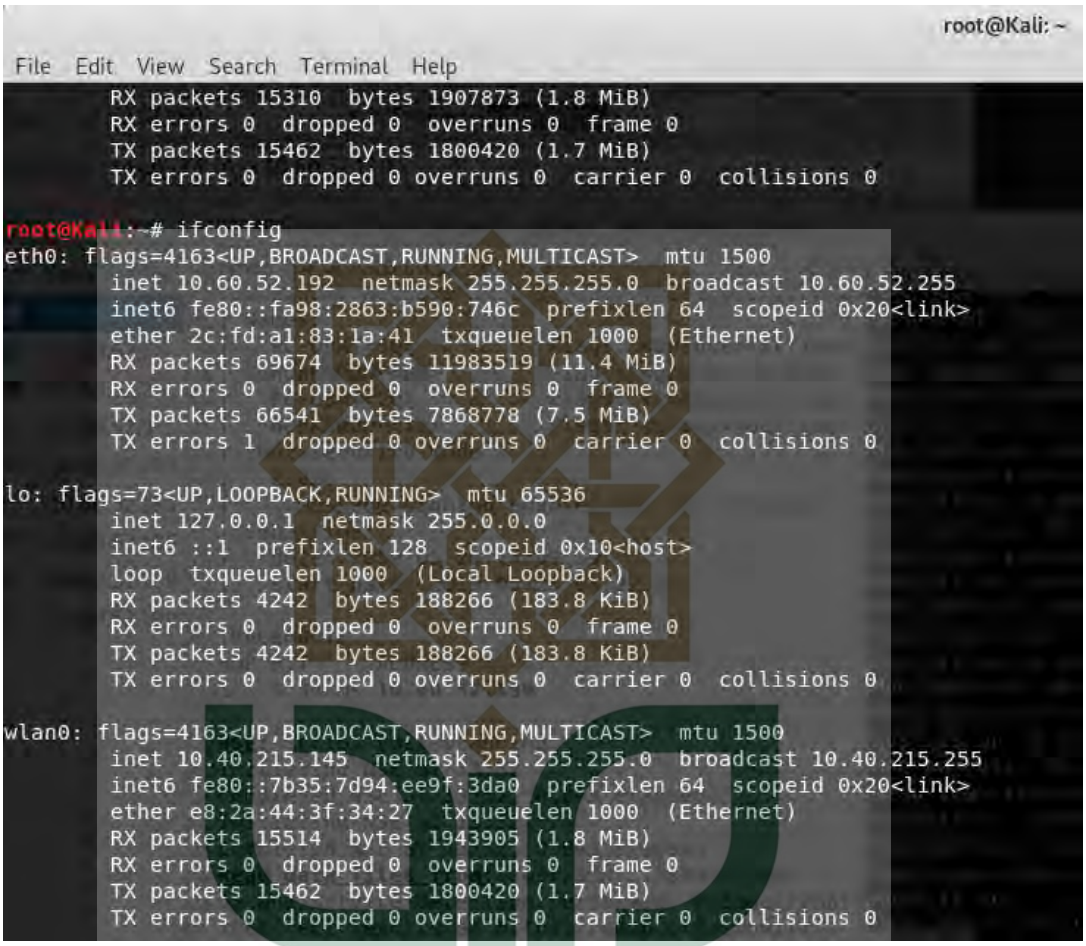






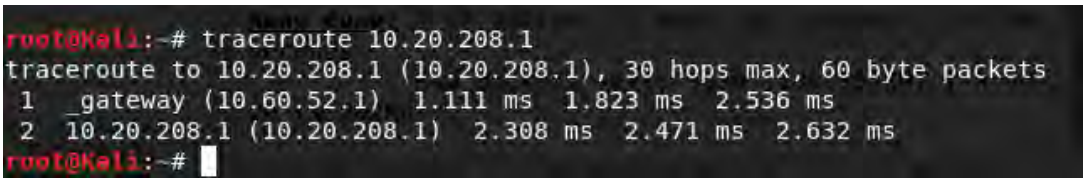
LAMPIRAN 8

Tampilan Hasil Dengan Ifconfig Pada Jaringan Laptop Kali Linux



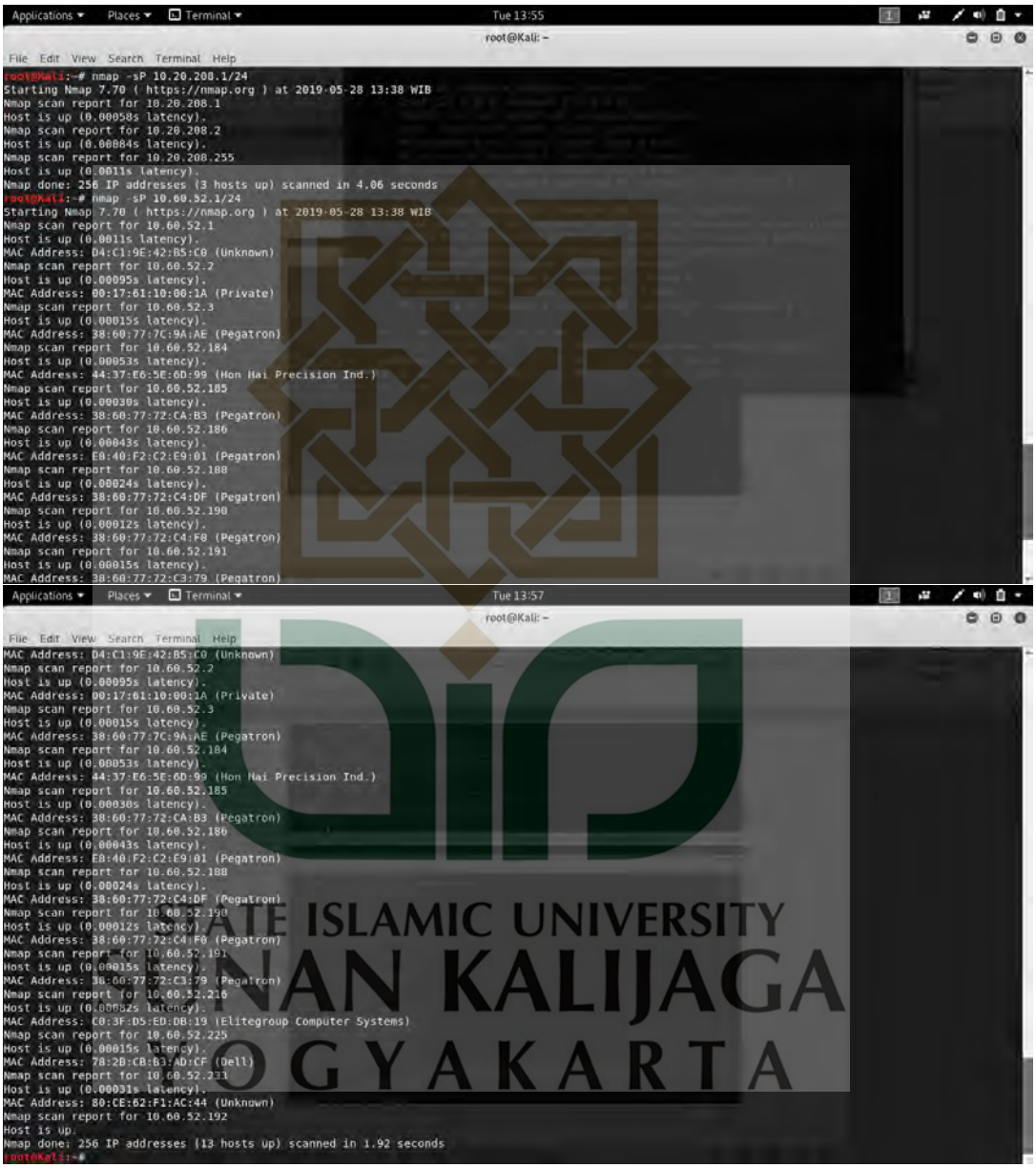
LAMPIRAN 9

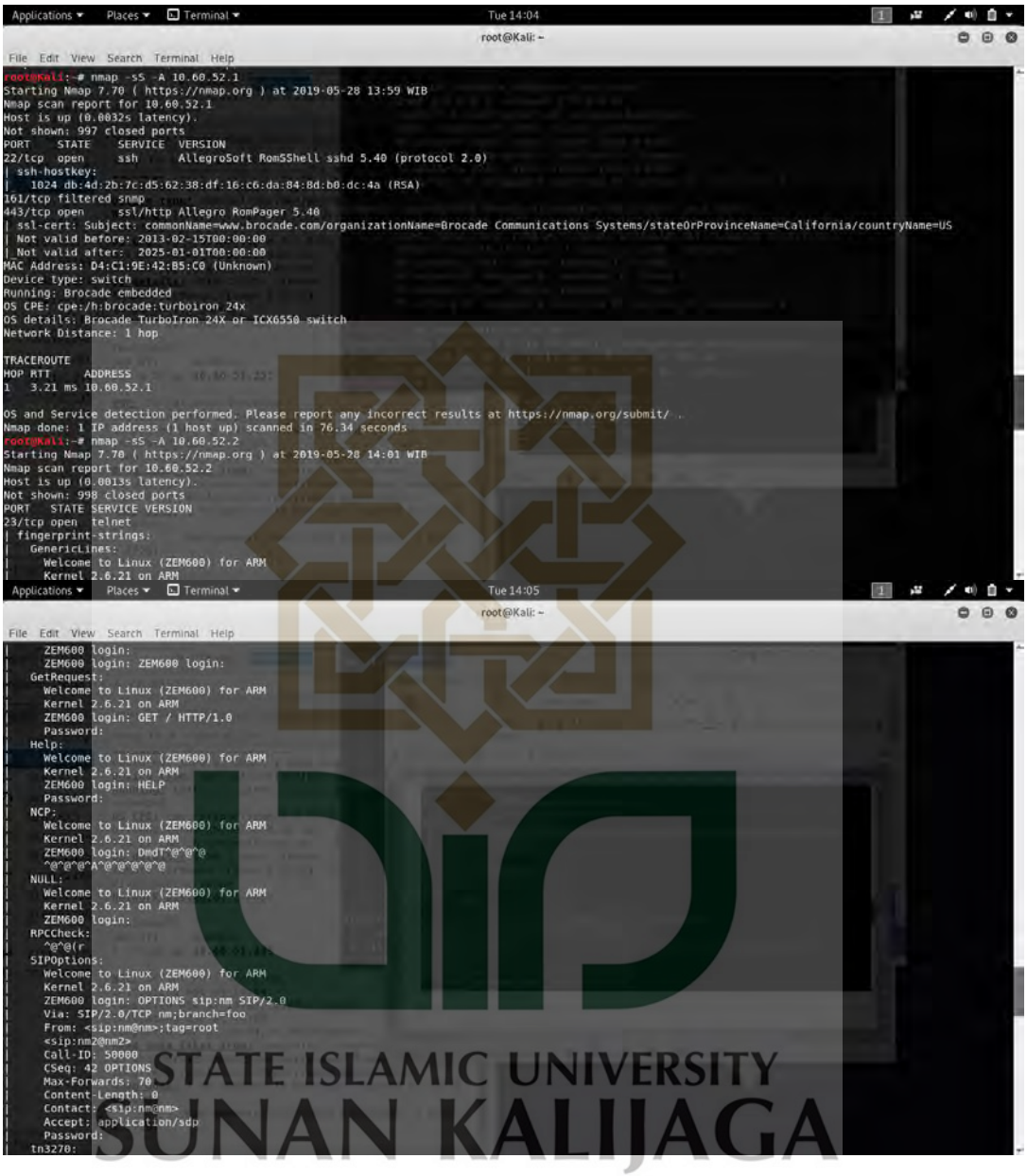
Tampilan Hasil Traceroute Pada Laptop Kali Linux

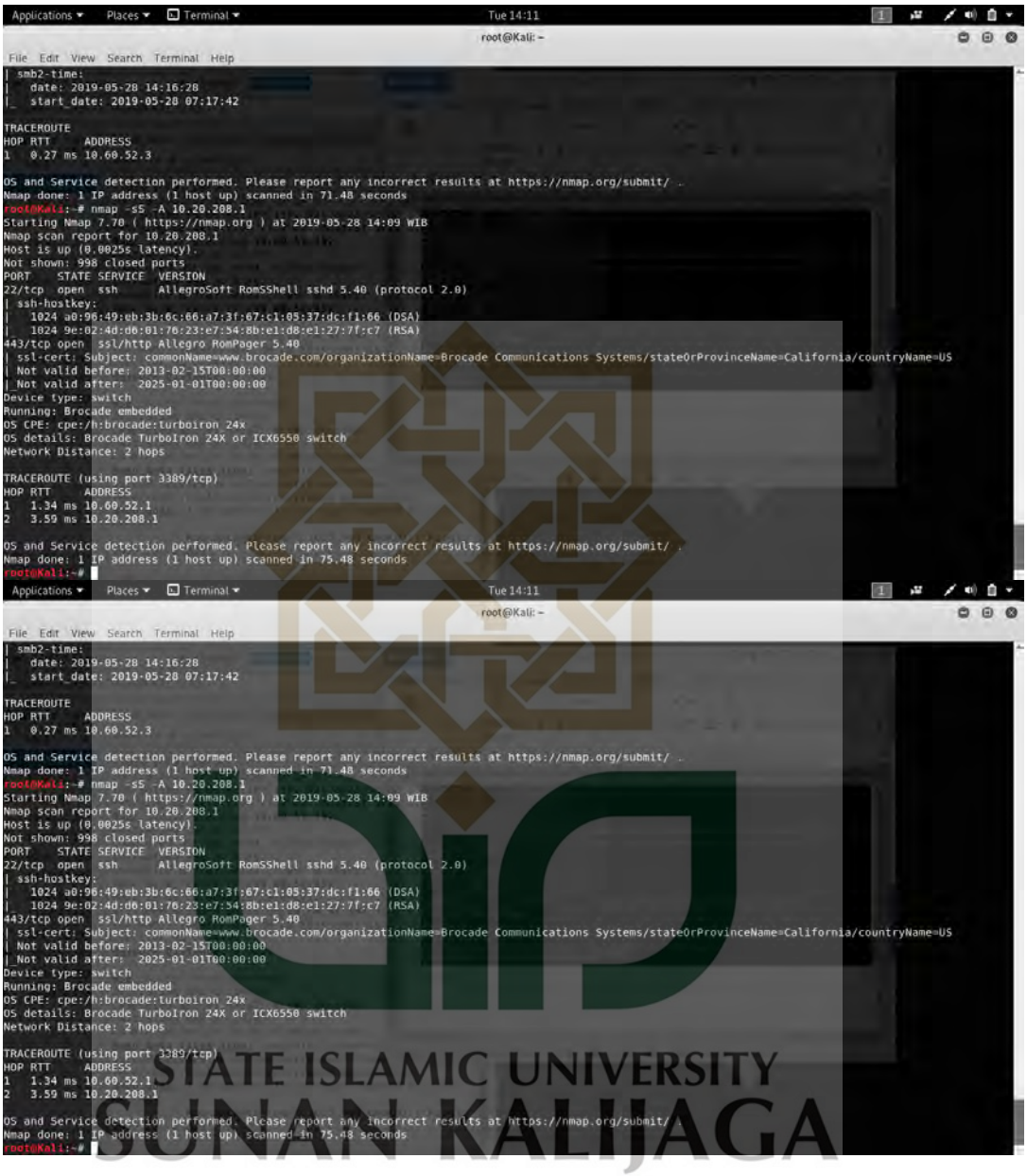


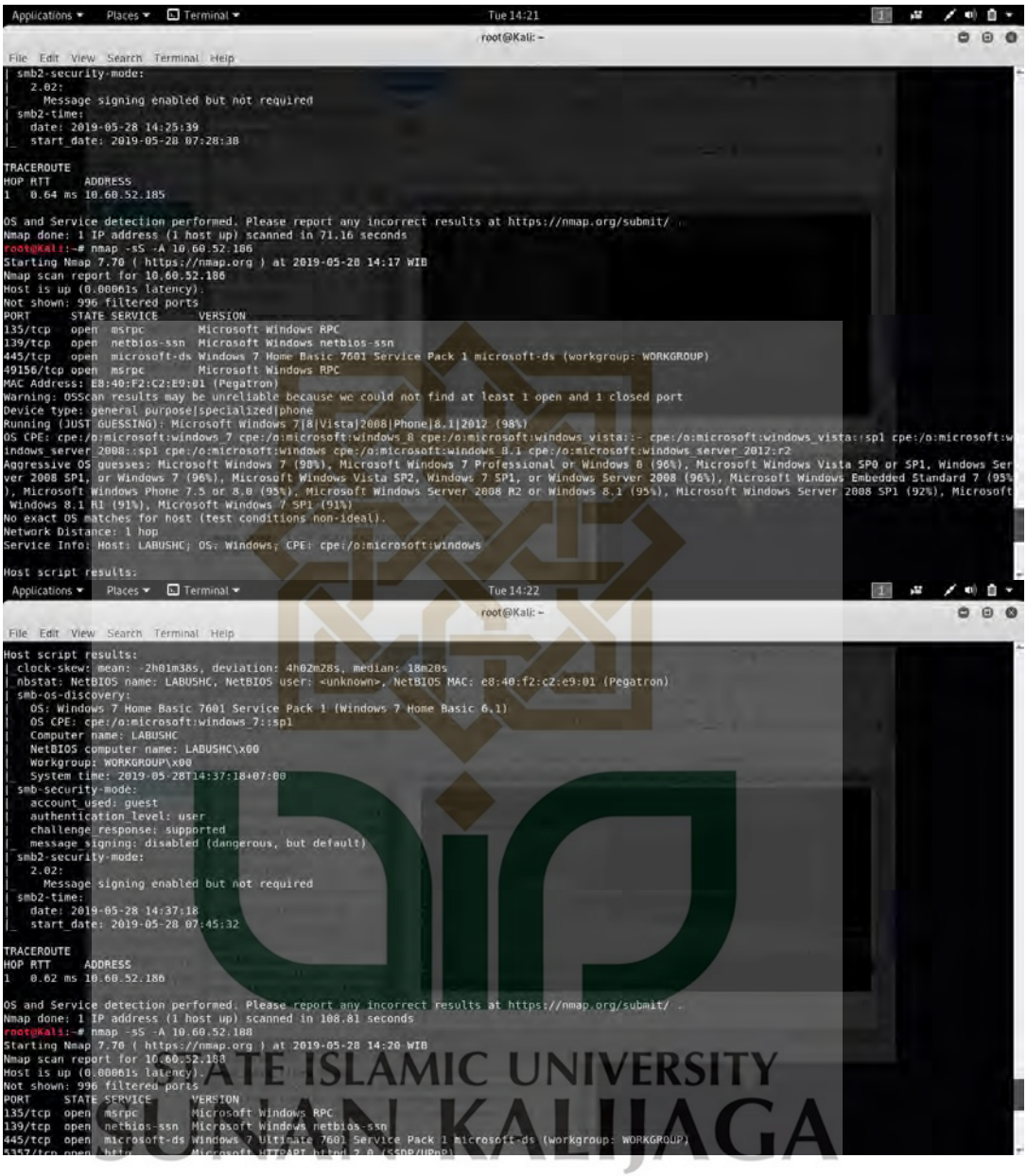
LAMPIRAN 10

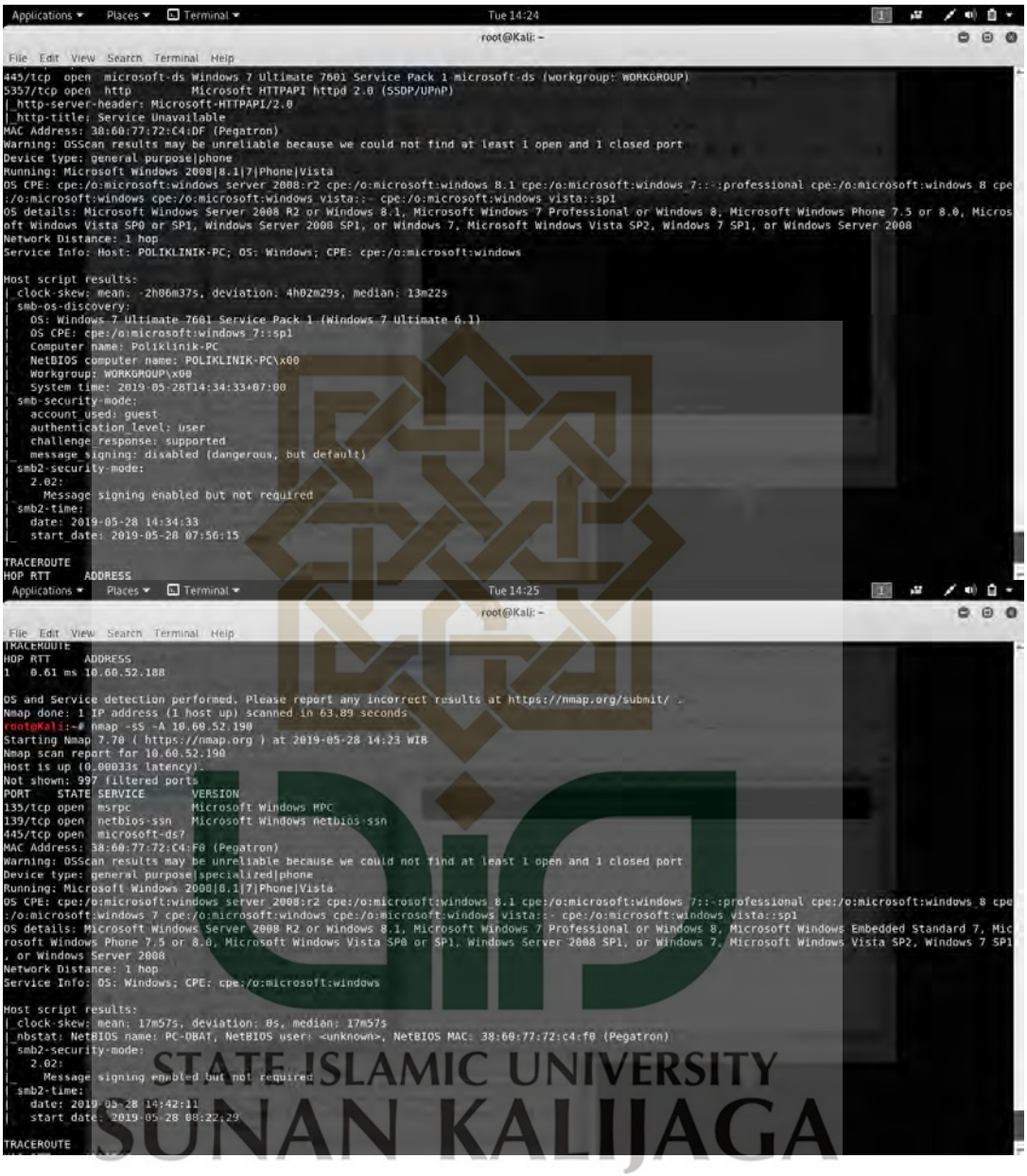
Tampilan Hasil *Scanning Port* Dengan Nmap Pada Jaringan Laptop Kali Linux

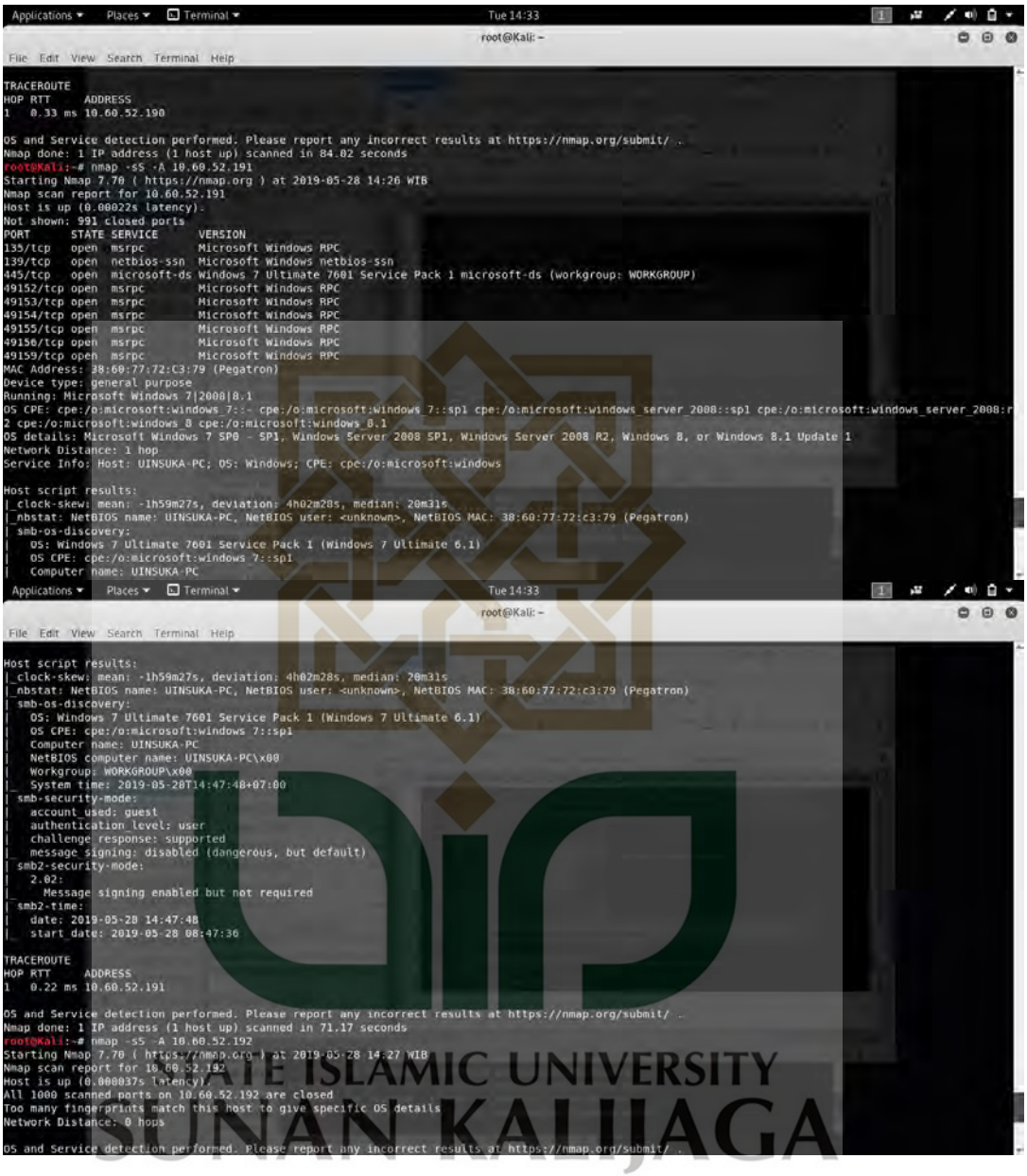


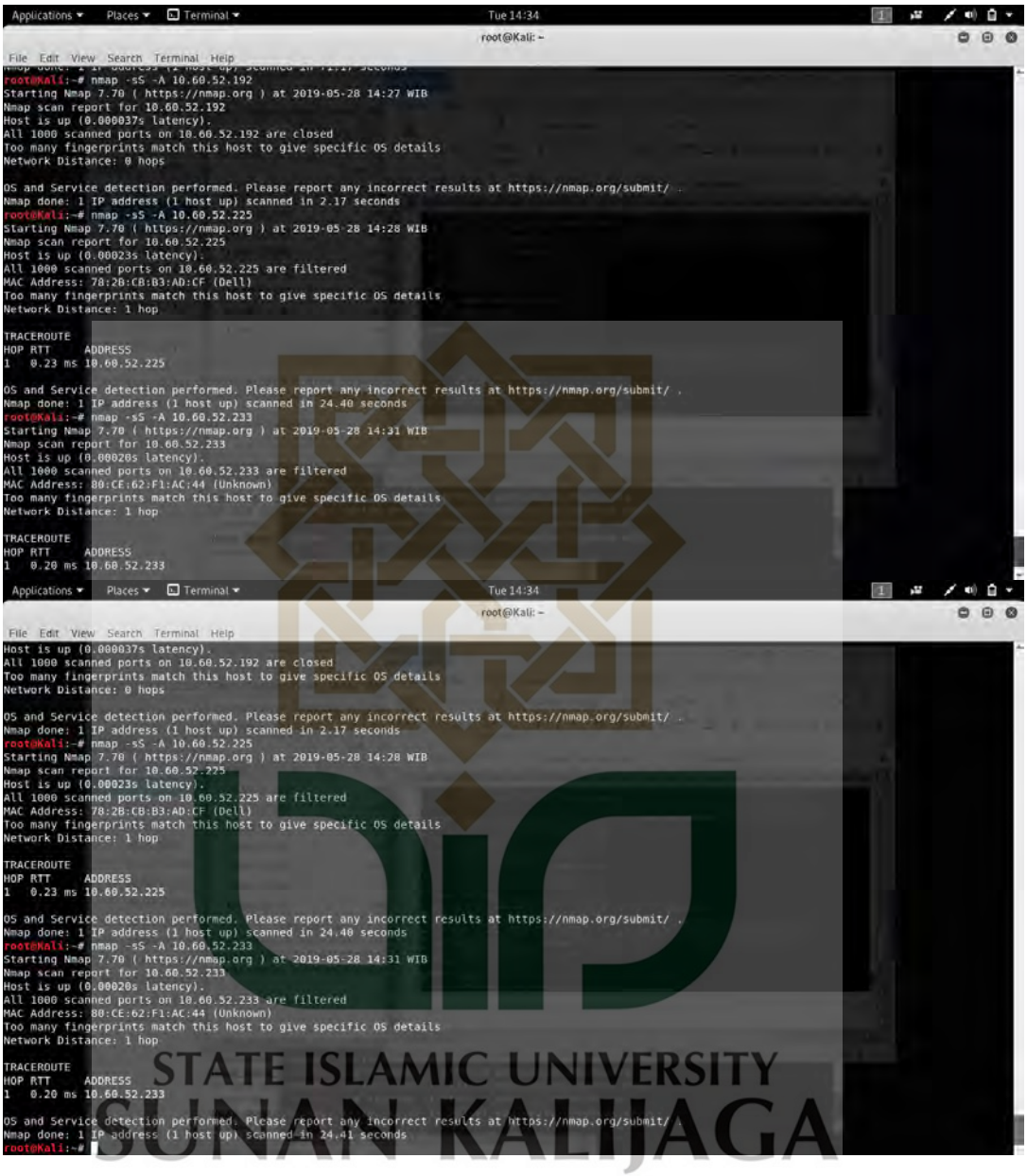






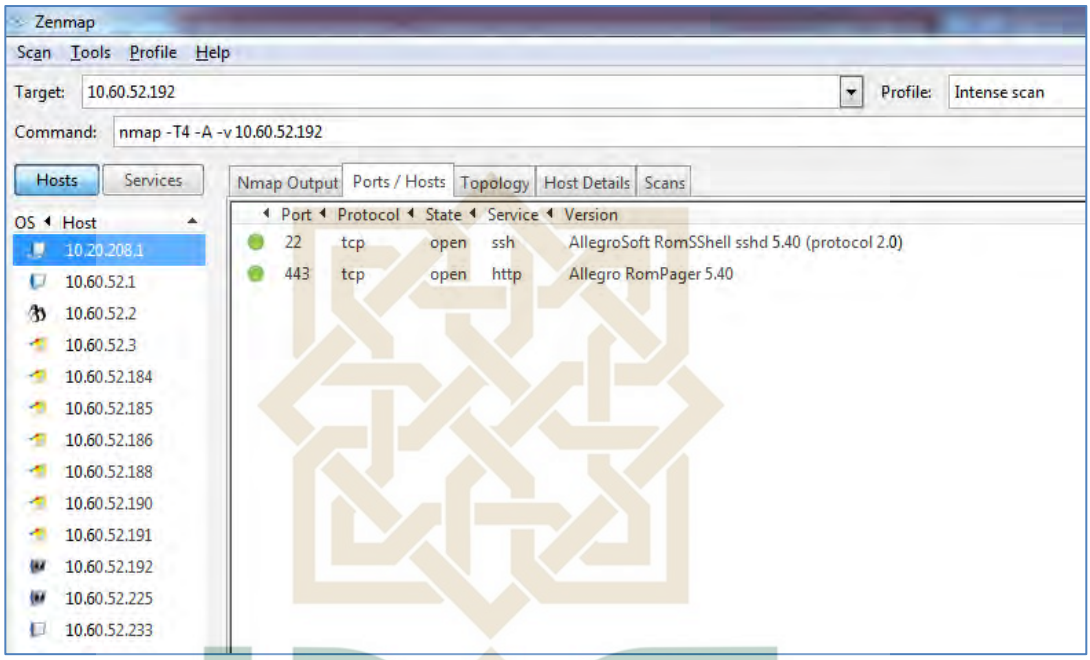


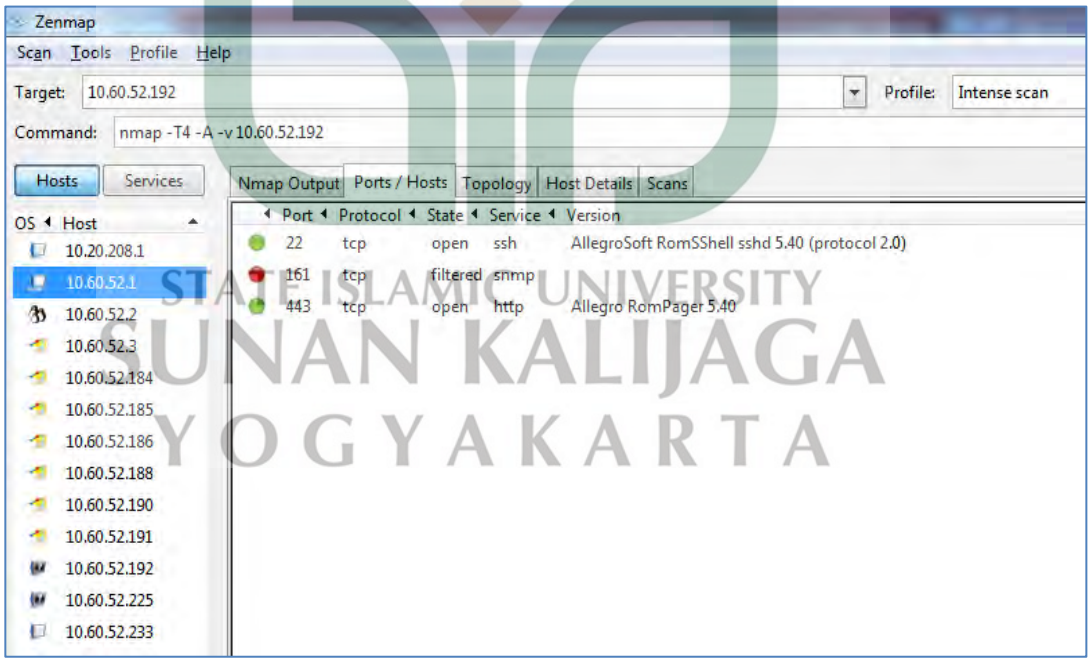


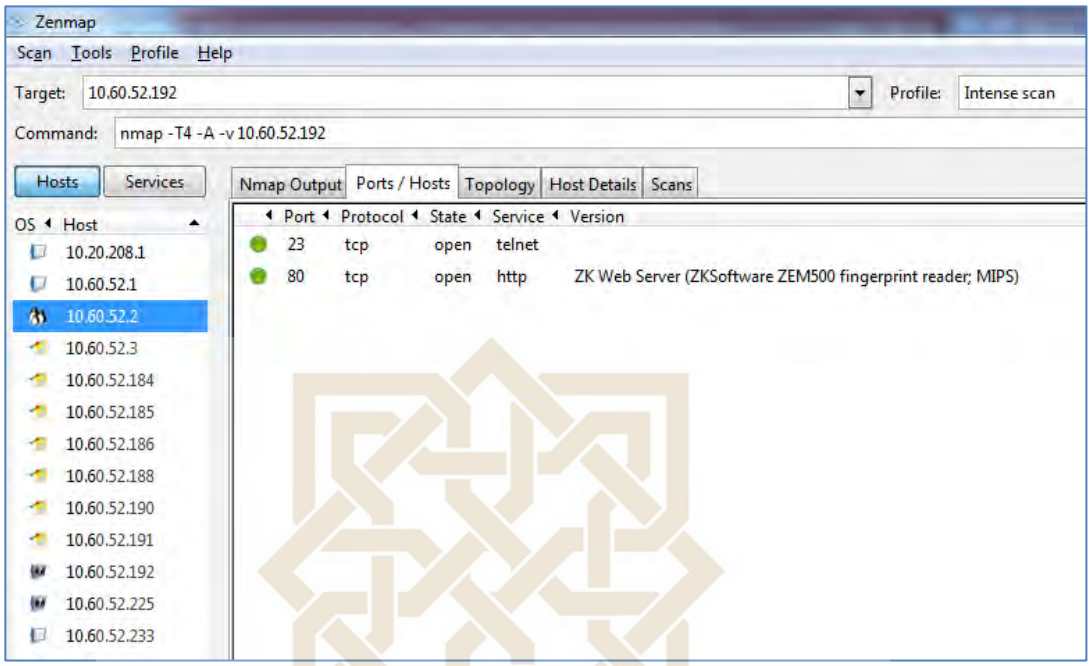


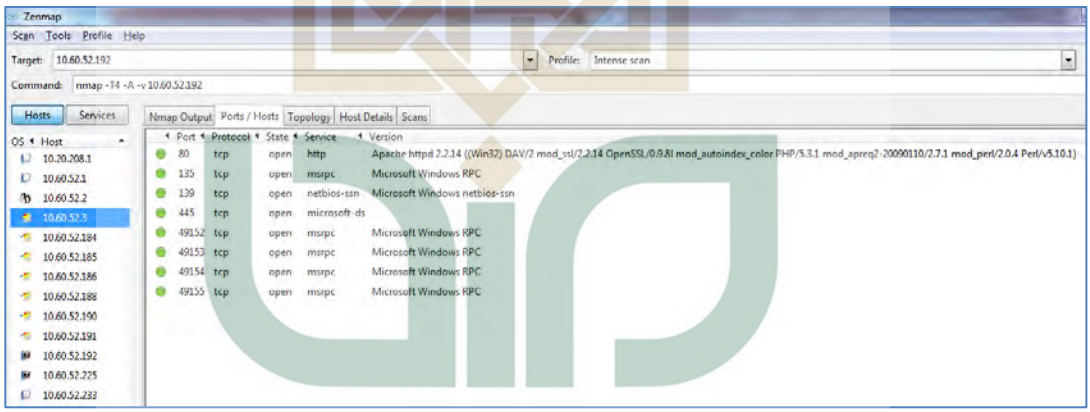
LAMPIRAN 11

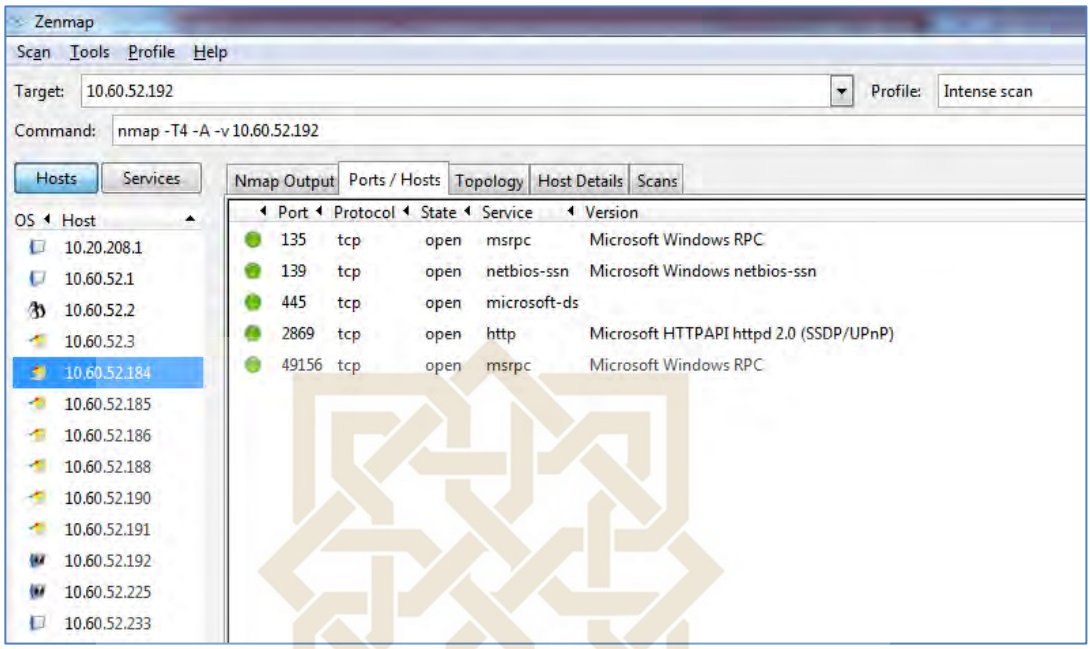
Tampilan Hasil Ip *Scanning* Dengan Zenmap Pada Jaringan Laptop Kali Linux

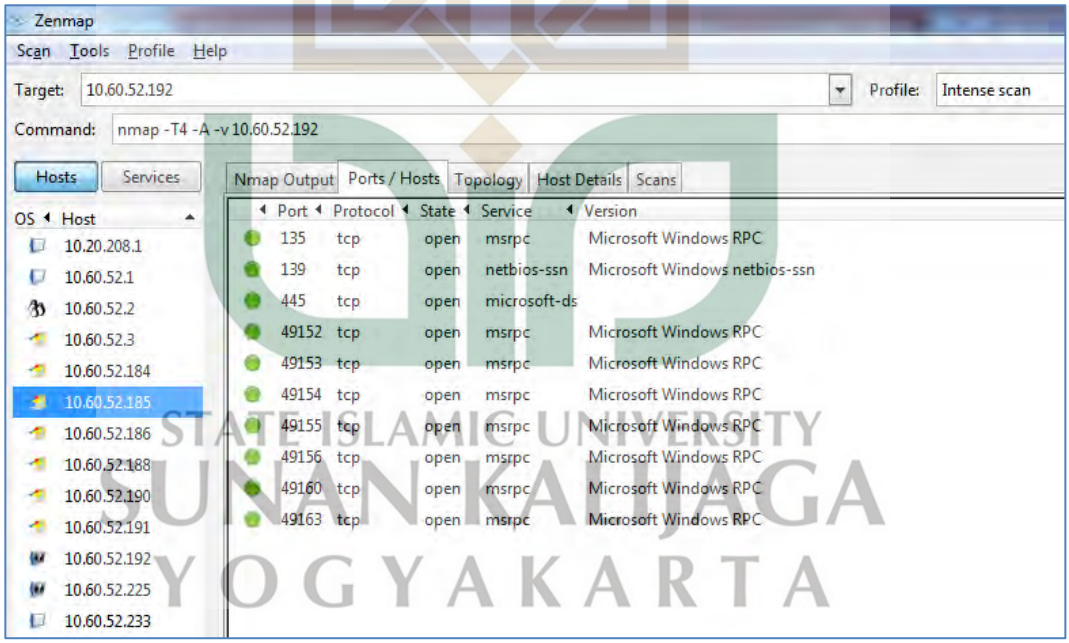


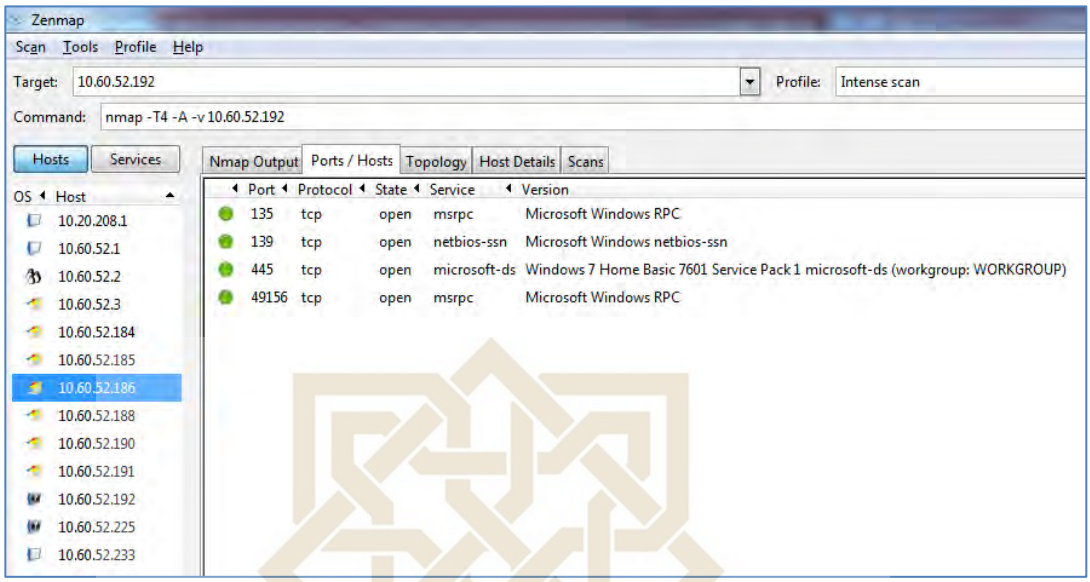


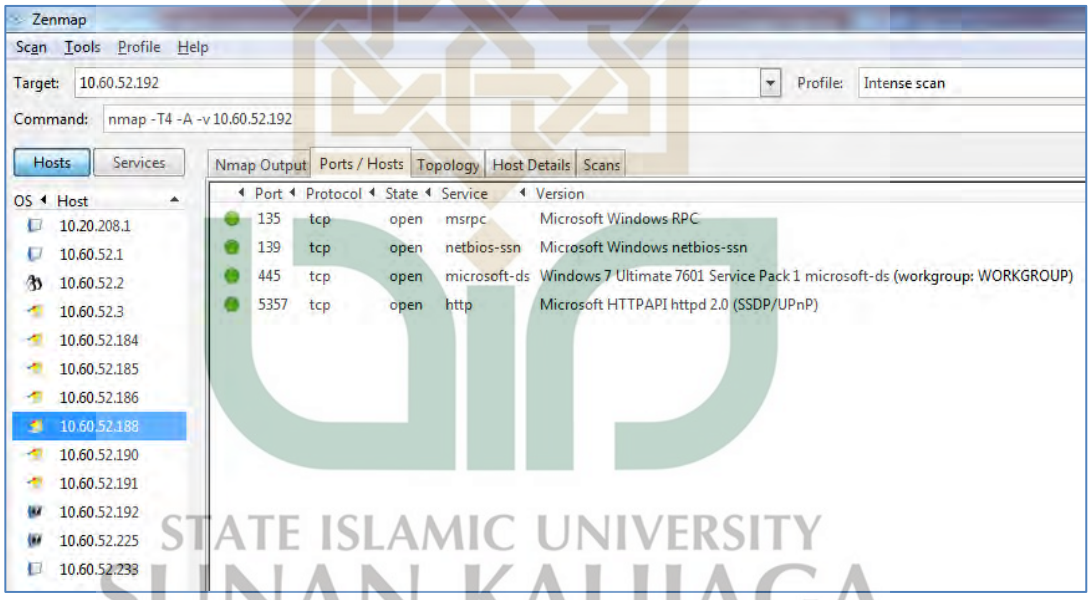


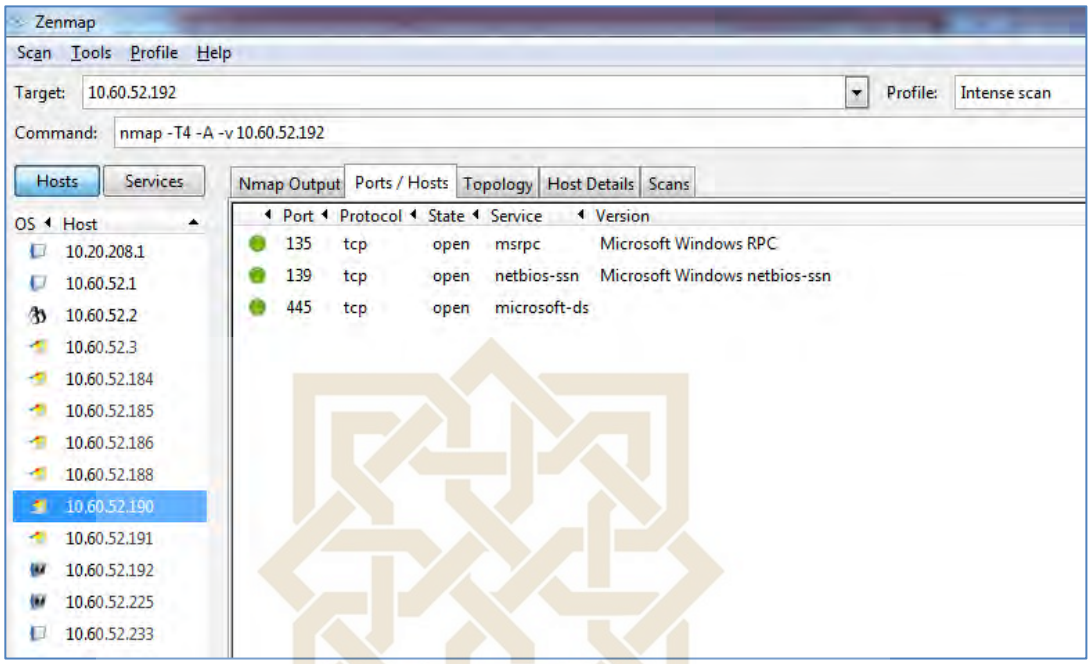


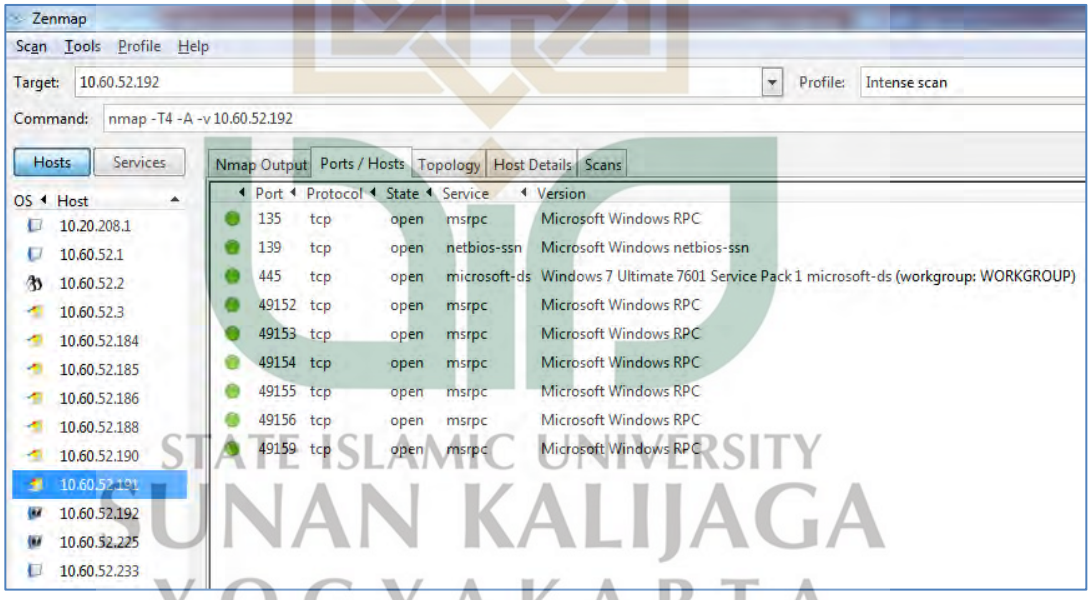


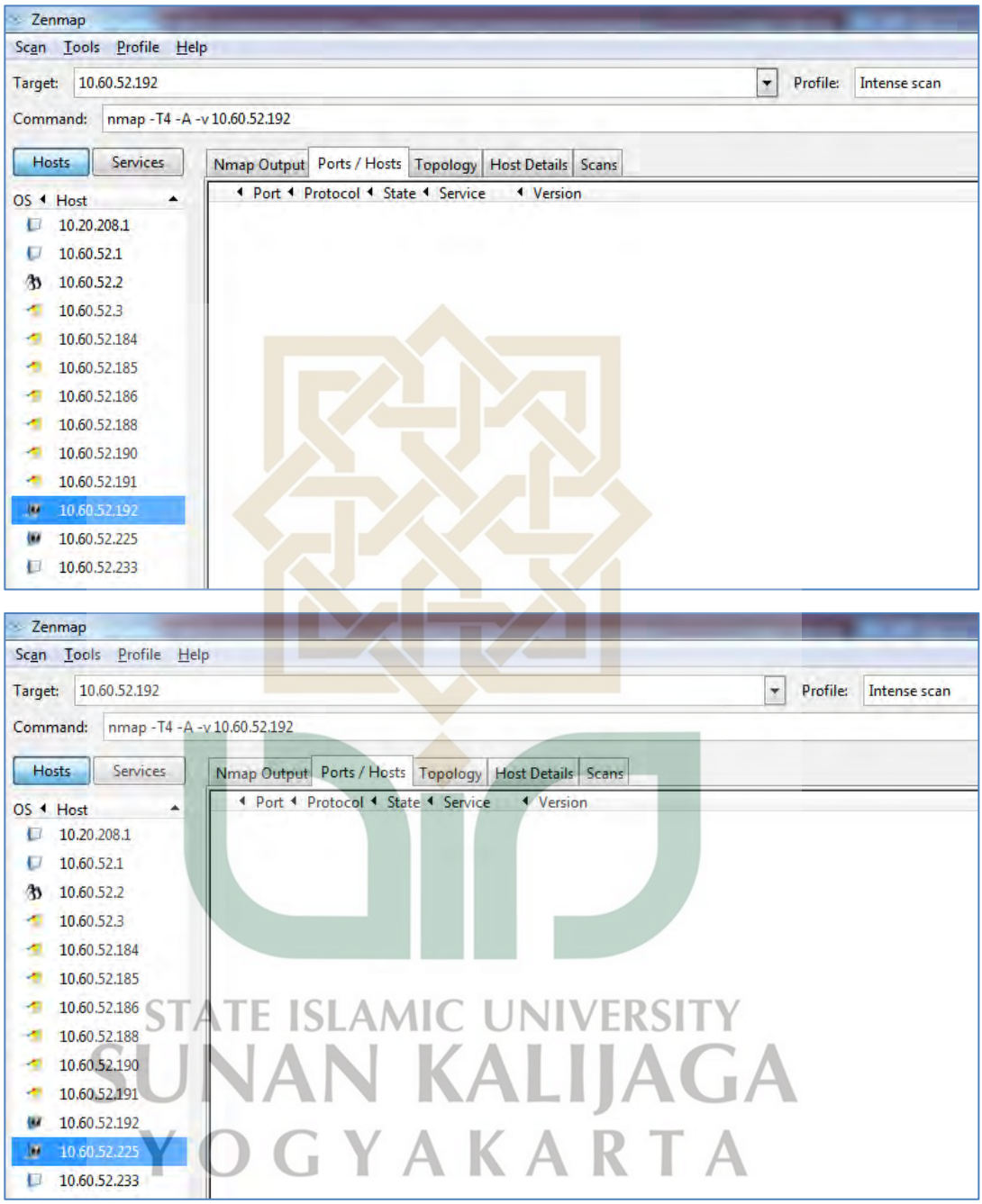


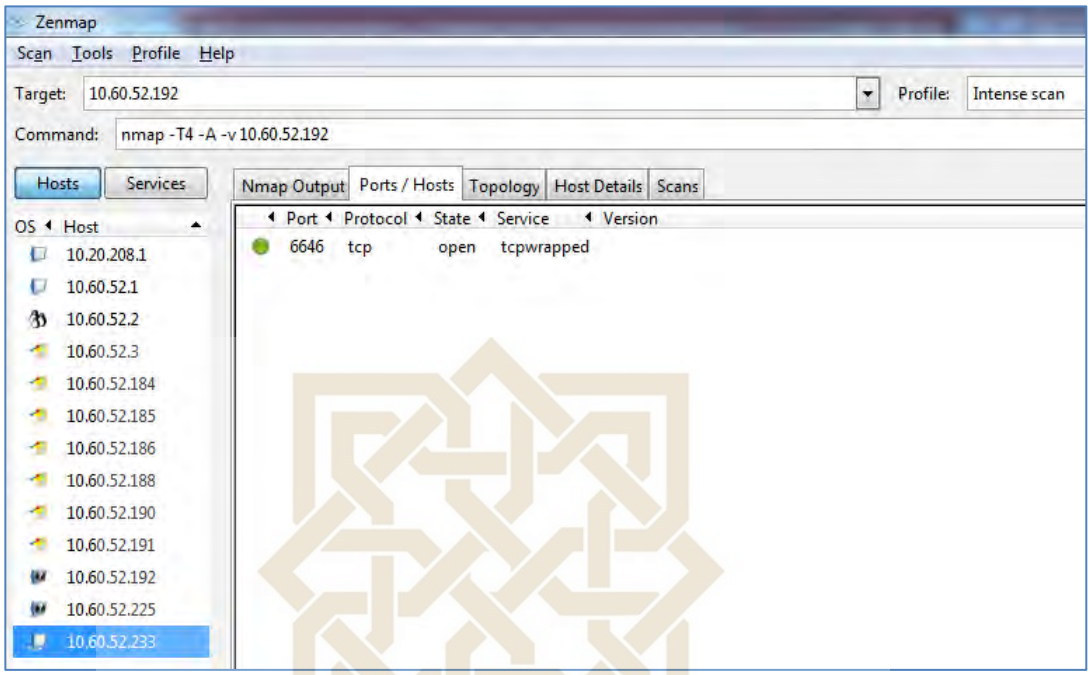






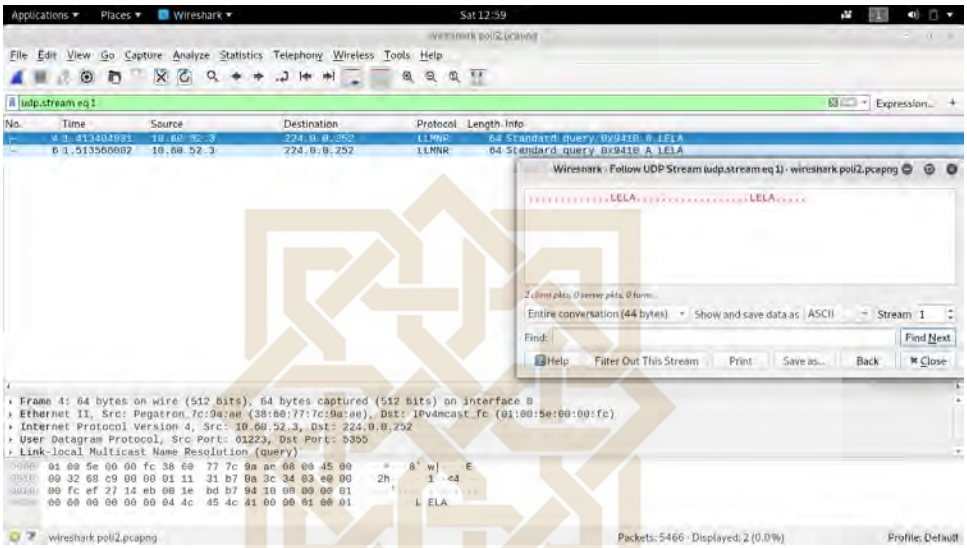


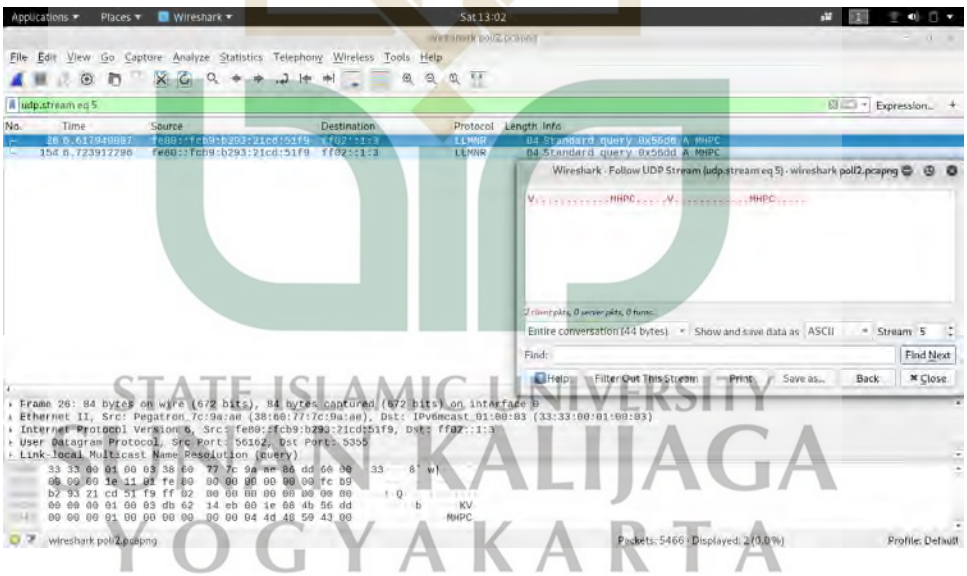


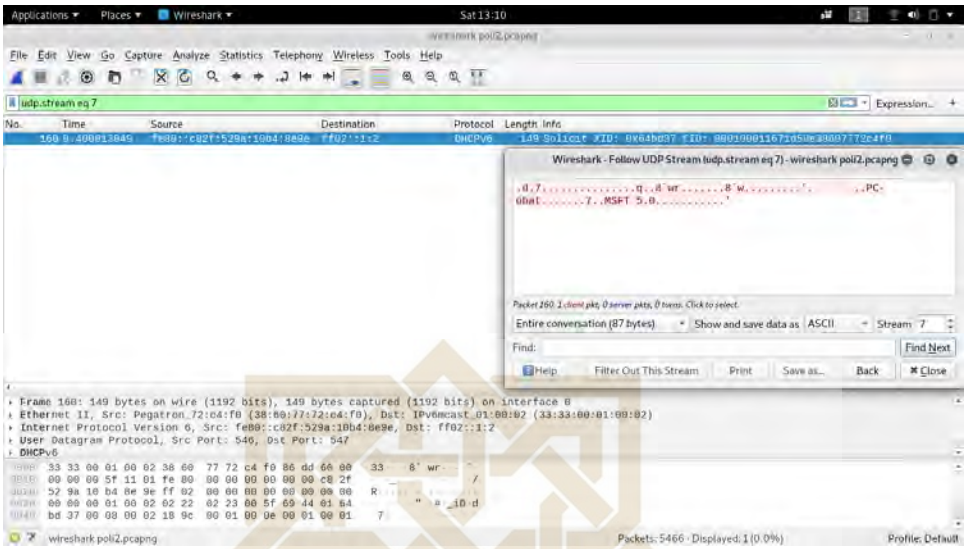


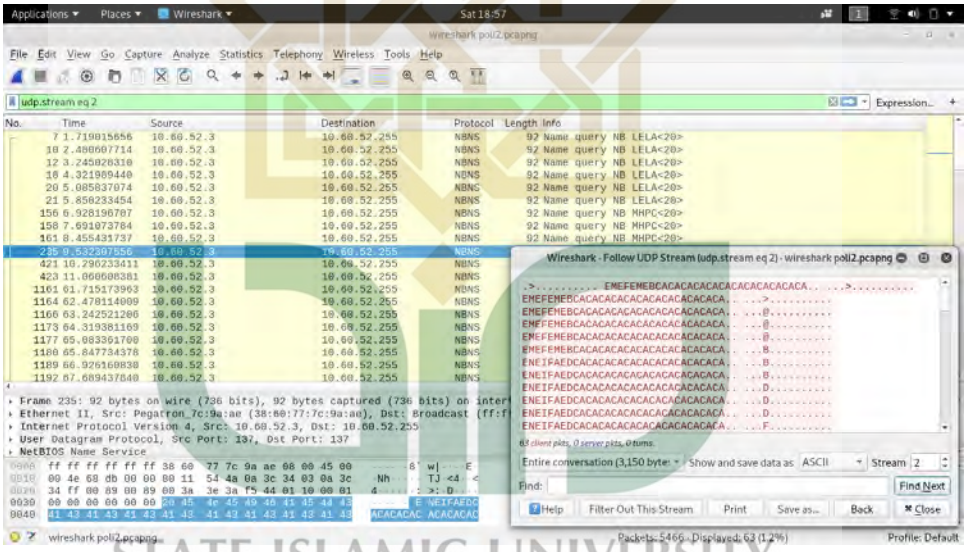
LAMPIRAN 12

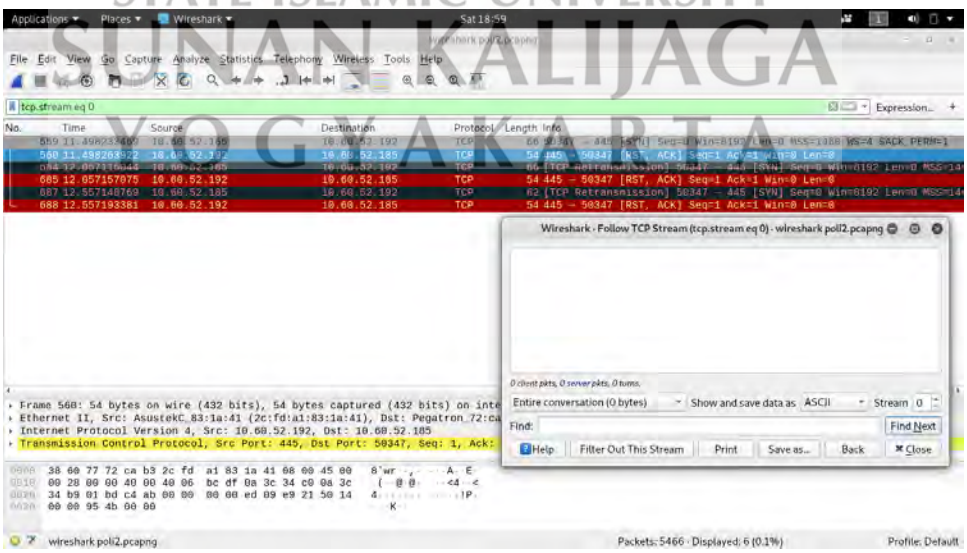
Tampilan Hasil Pembacaan Paket Data (TCP dan UDP Stream) Dengan Wireshark Pada Jaringan Laptop Kali Linux

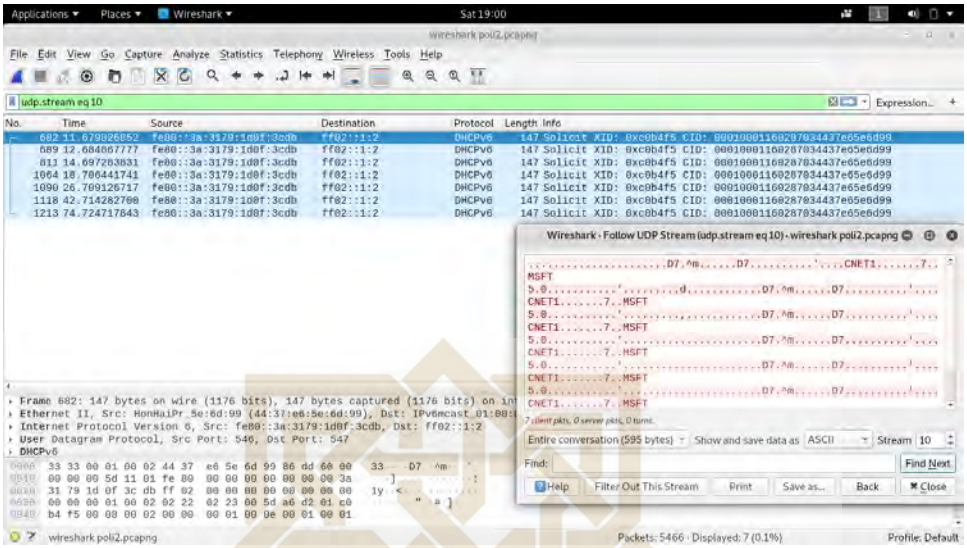


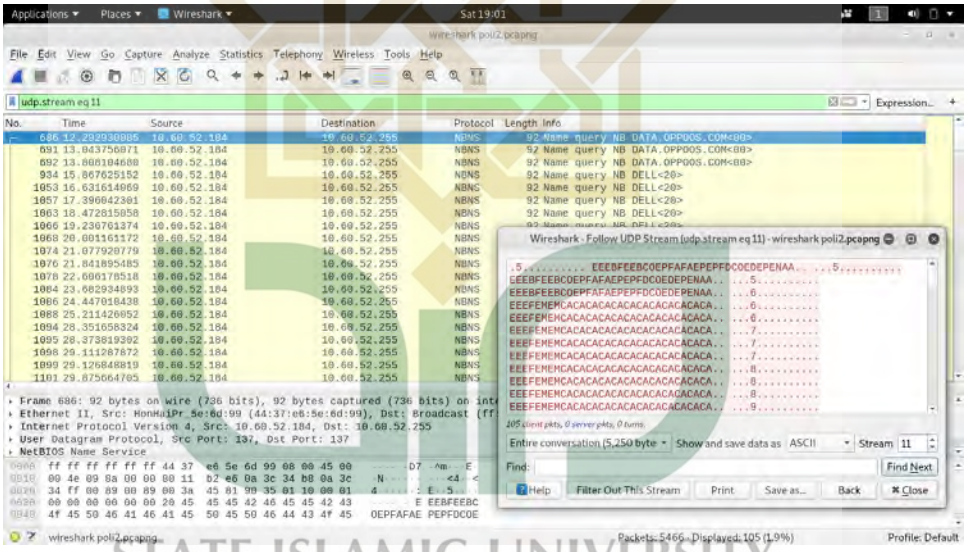


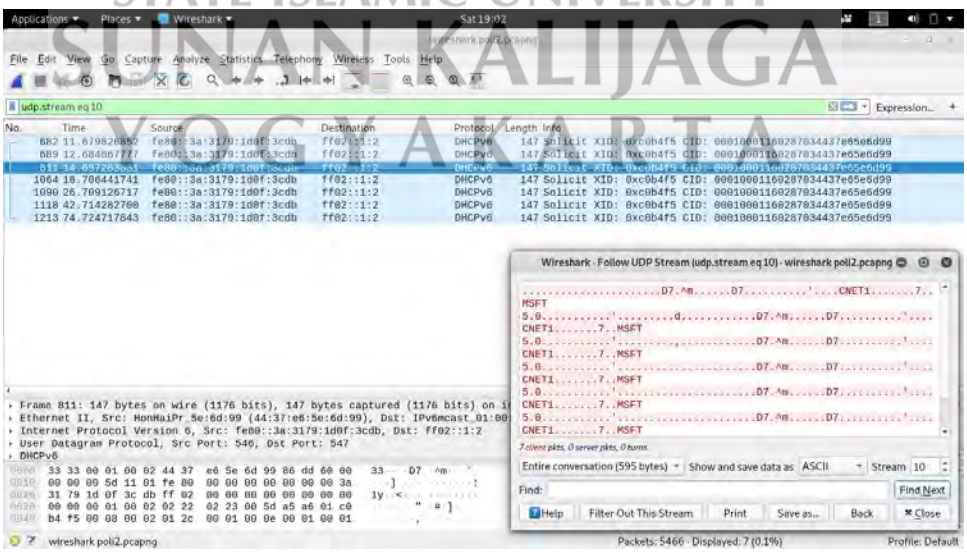


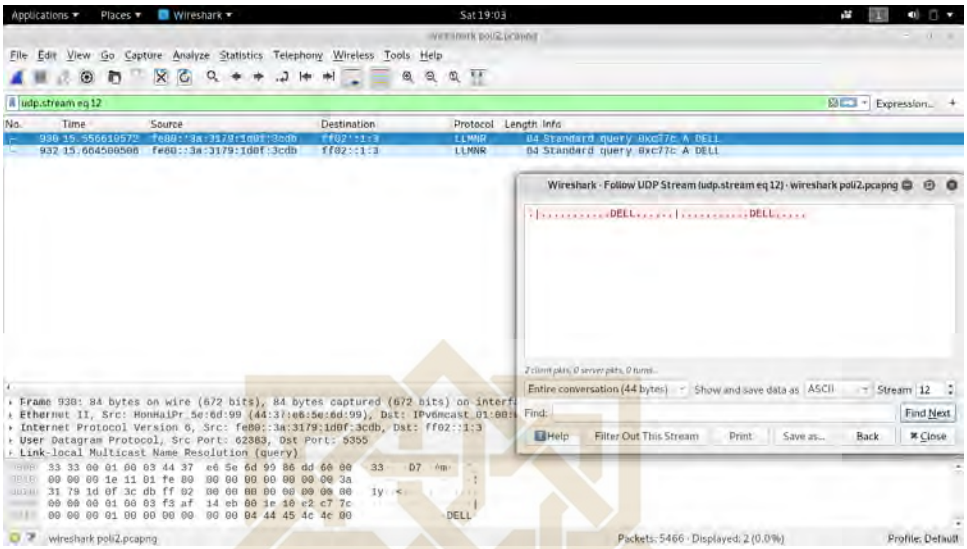


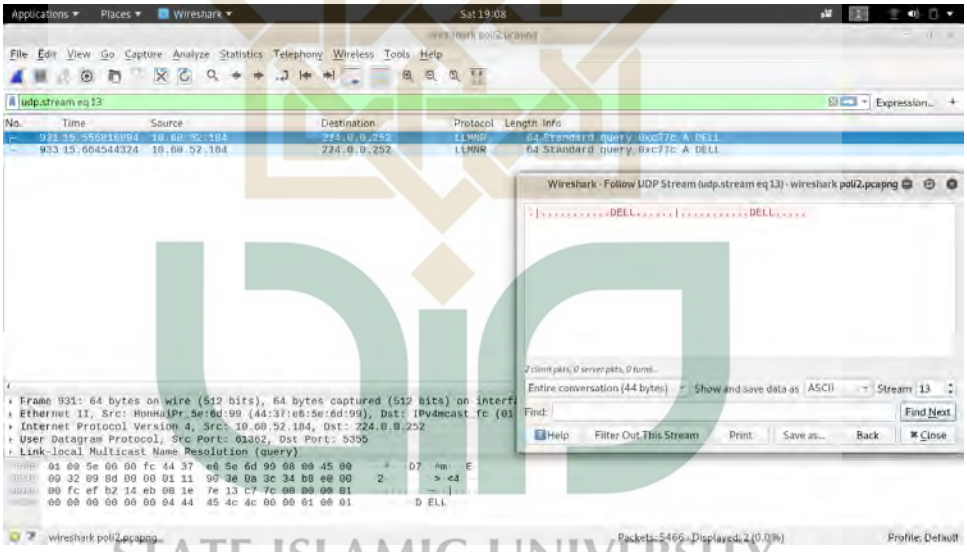


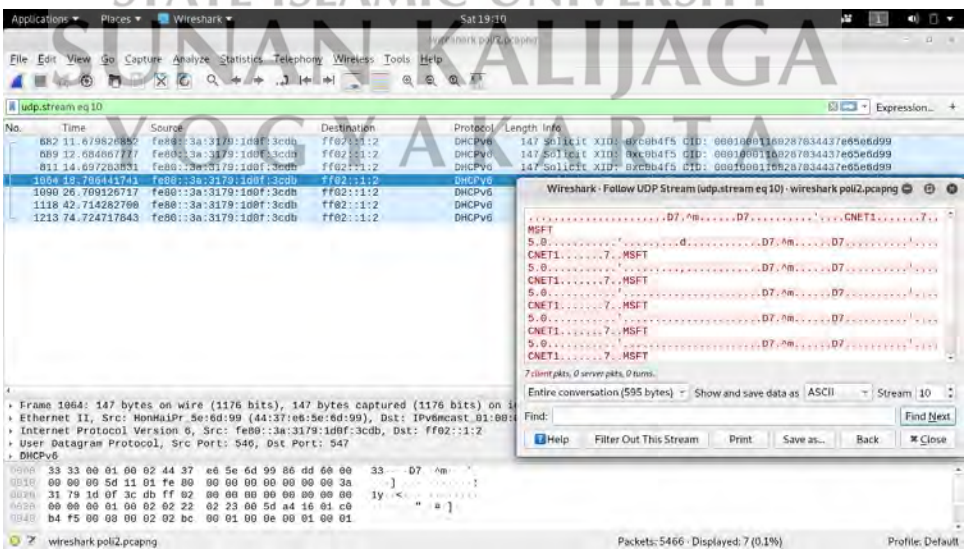


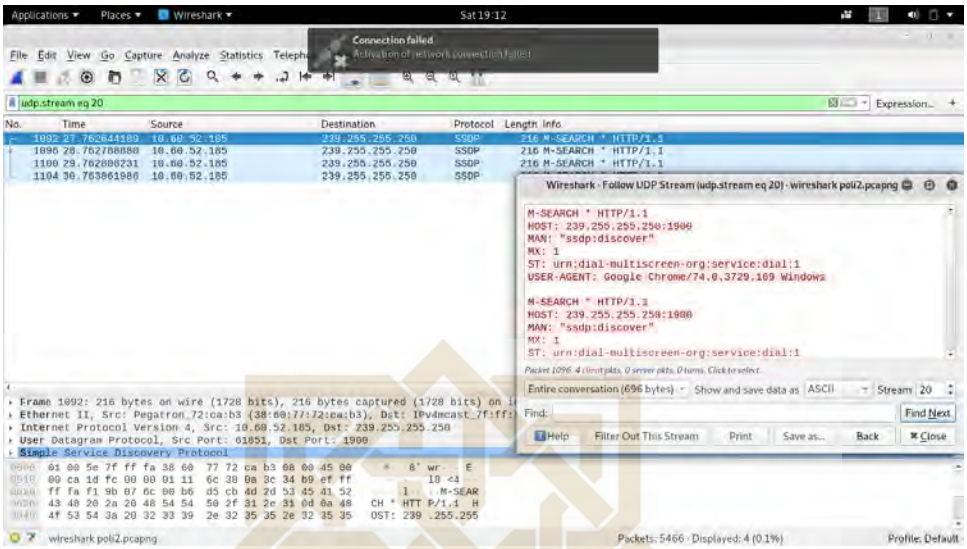


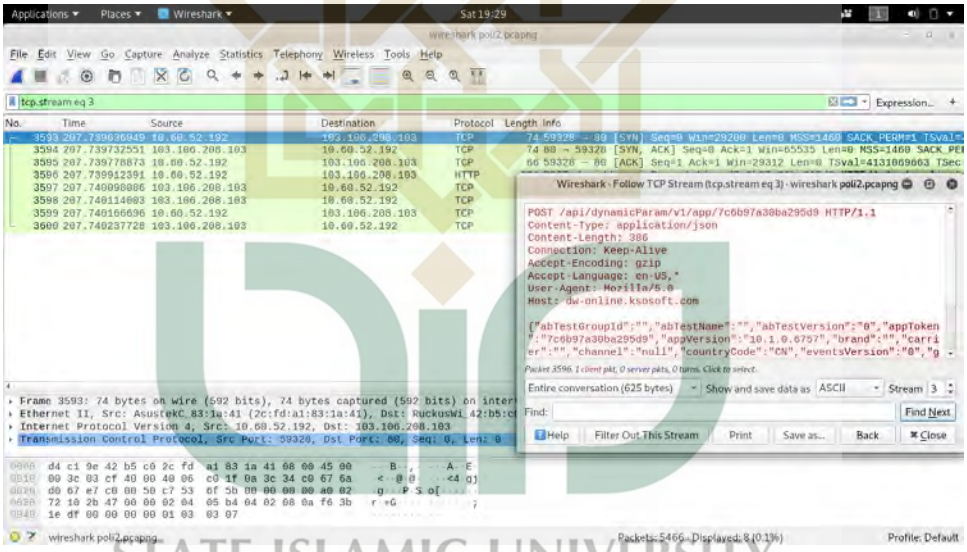


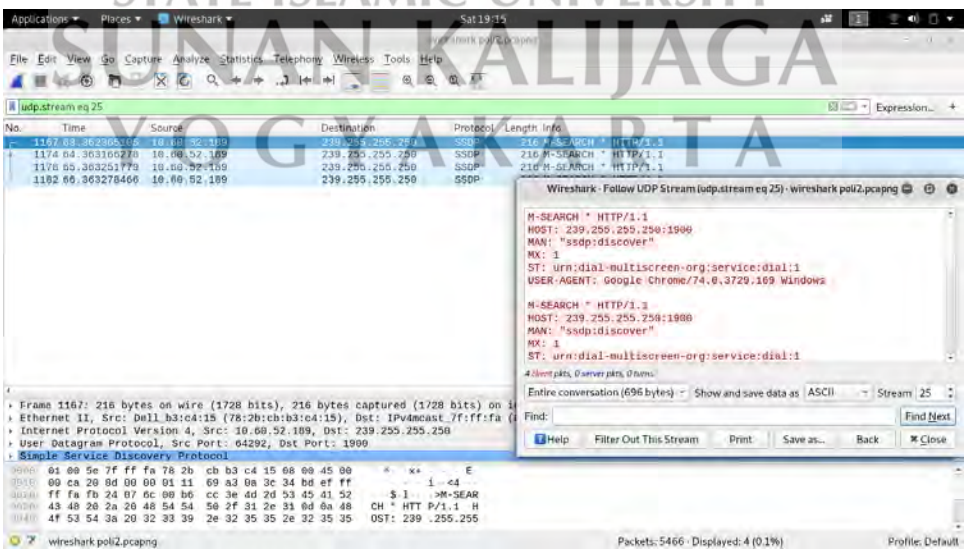


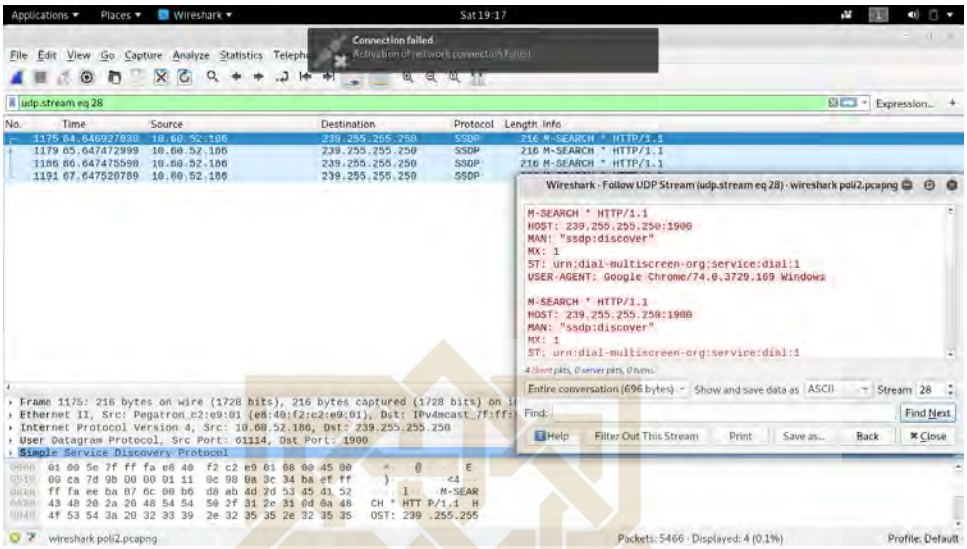


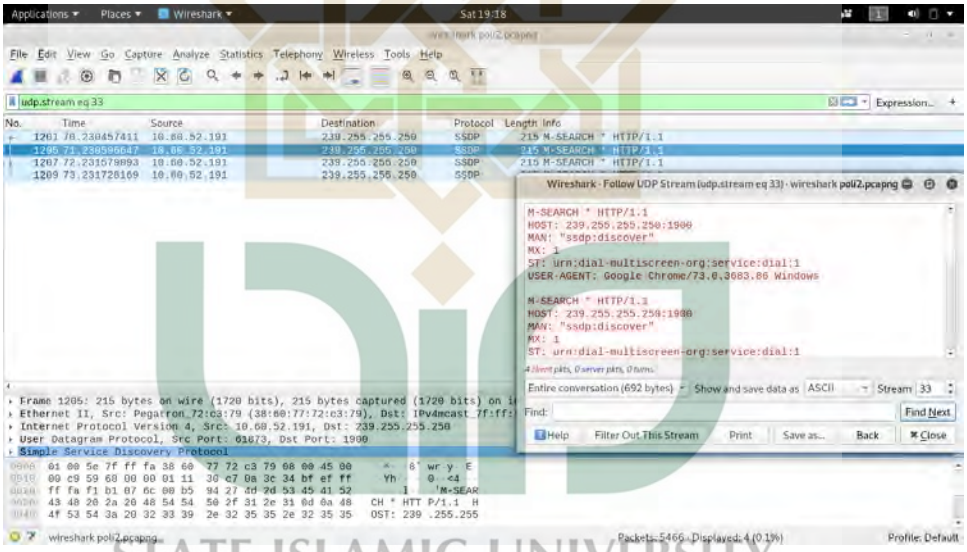


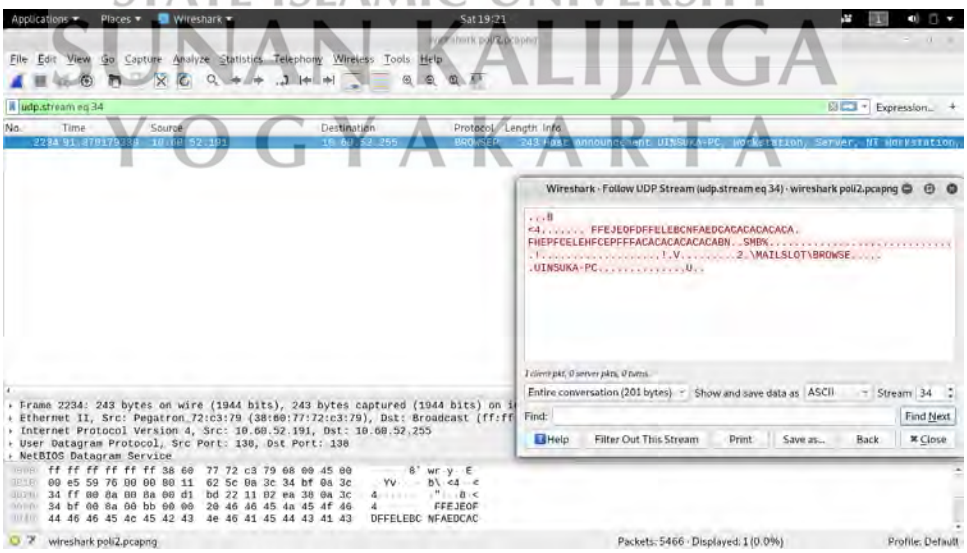


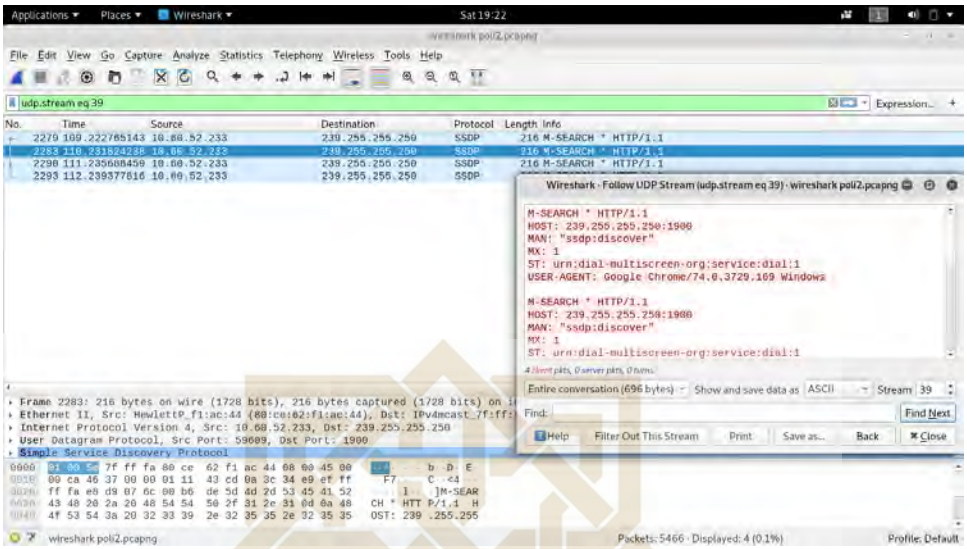


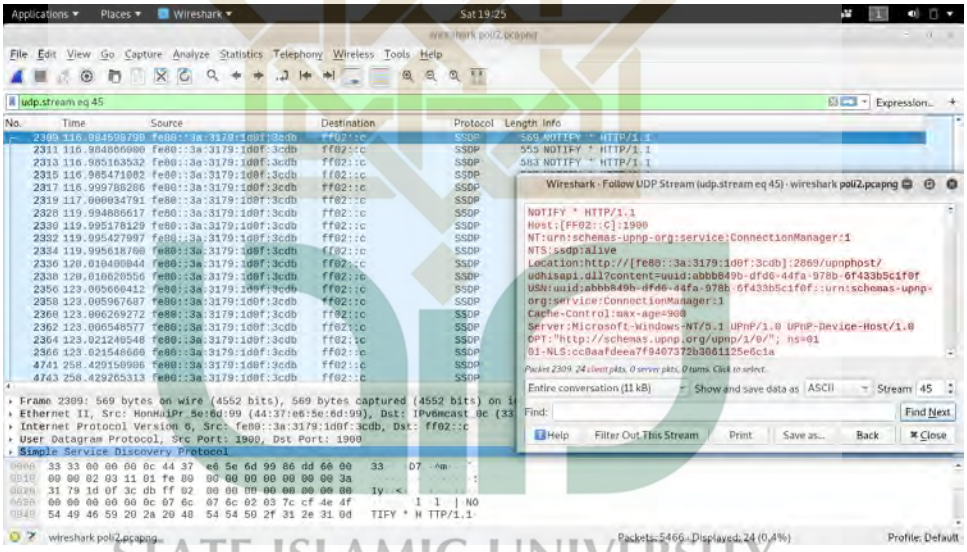


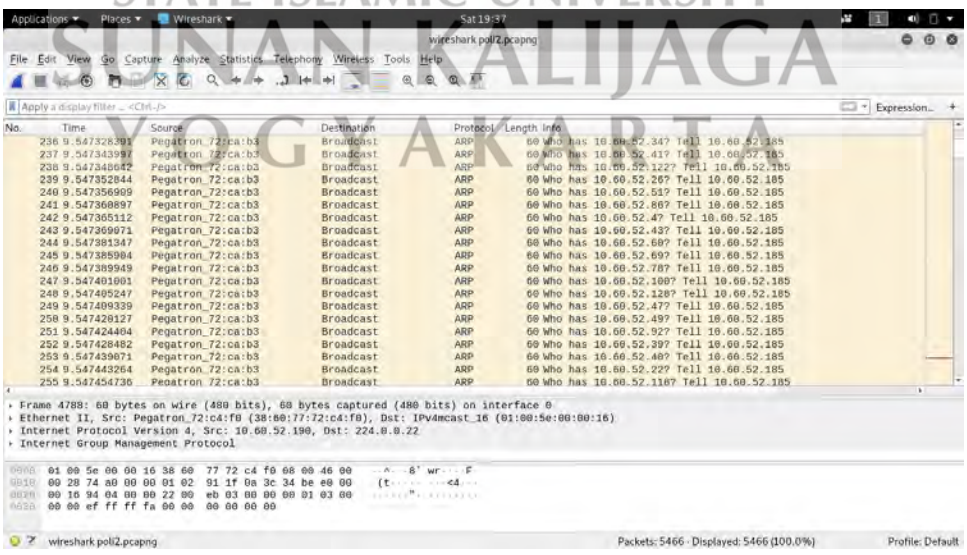






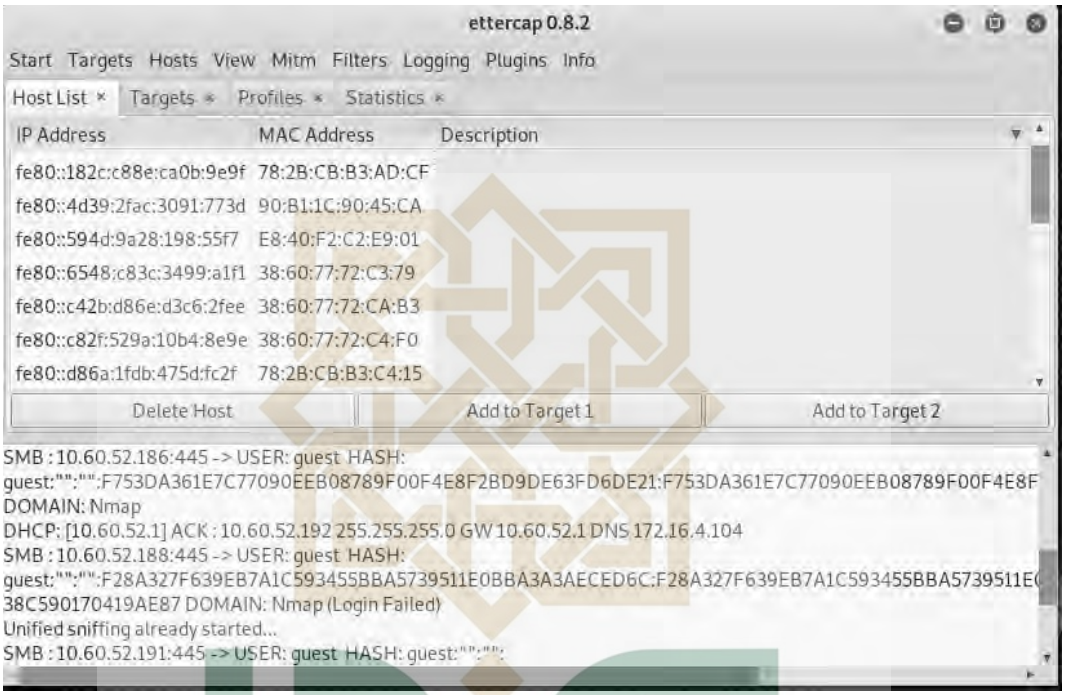


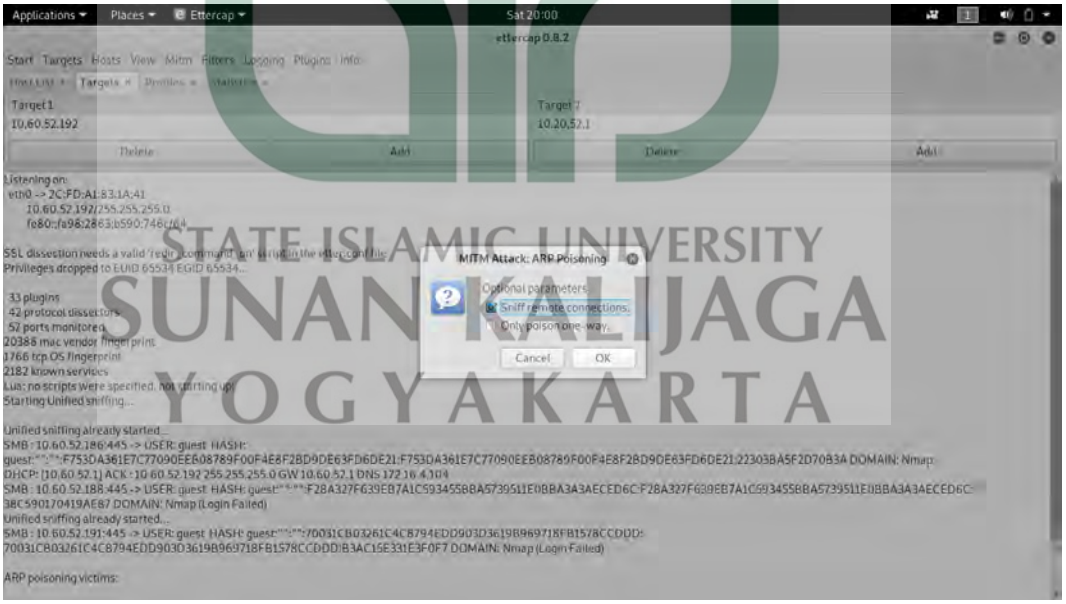


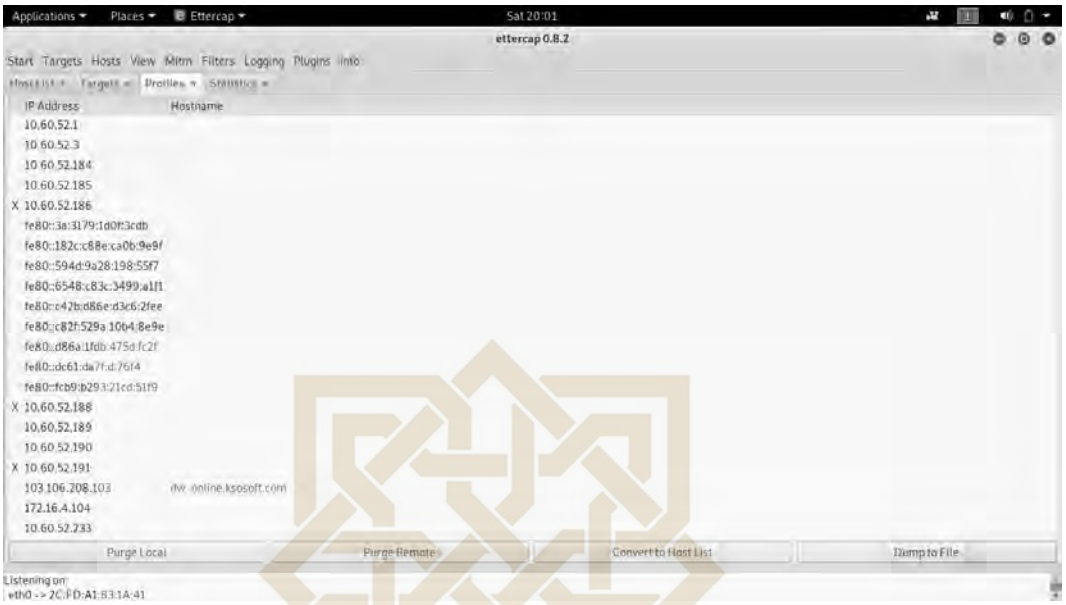


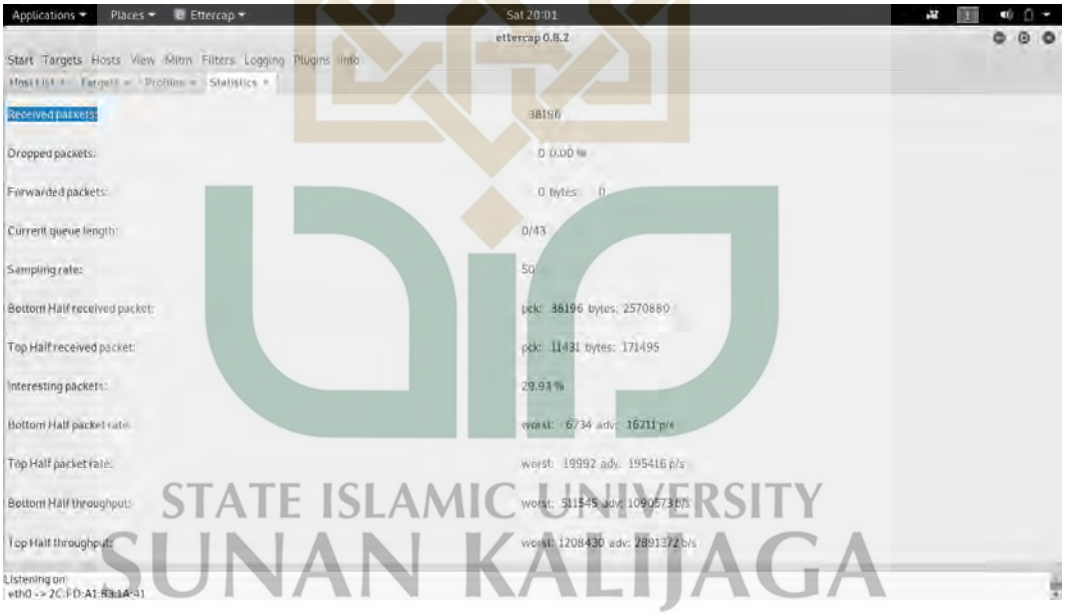
LAMPIRAN 13

Tampilan Percobaan Penyerangan Mitm ARP *Poisoning* Dengan Ettercap Pada Jaringan Laptop Kali Linux



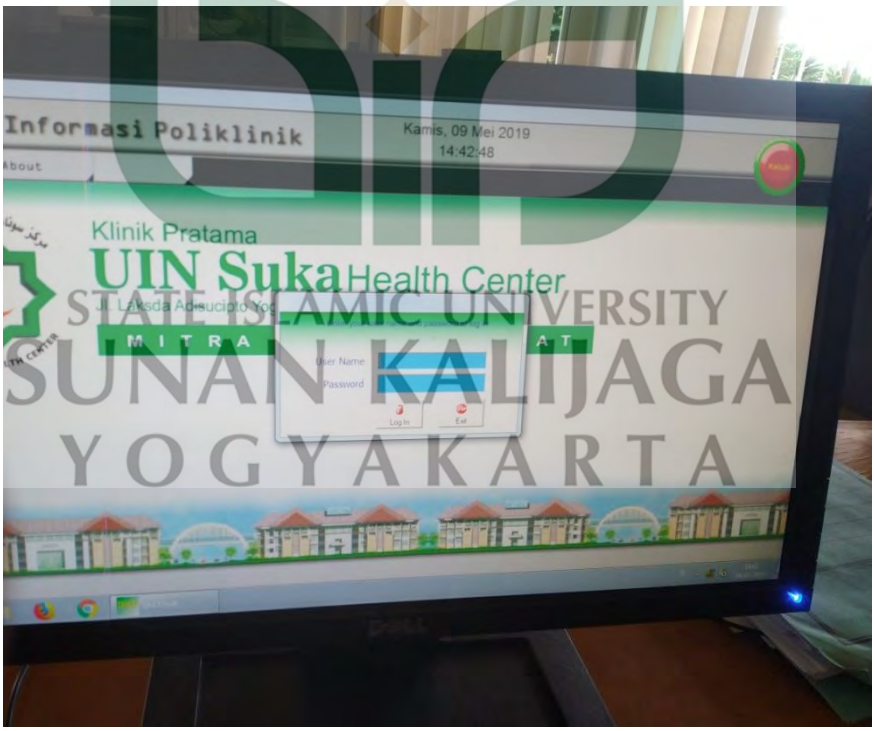






LAMPIRAN 14

Gambar Sistem Informasi dan Administrasi yang diaudit

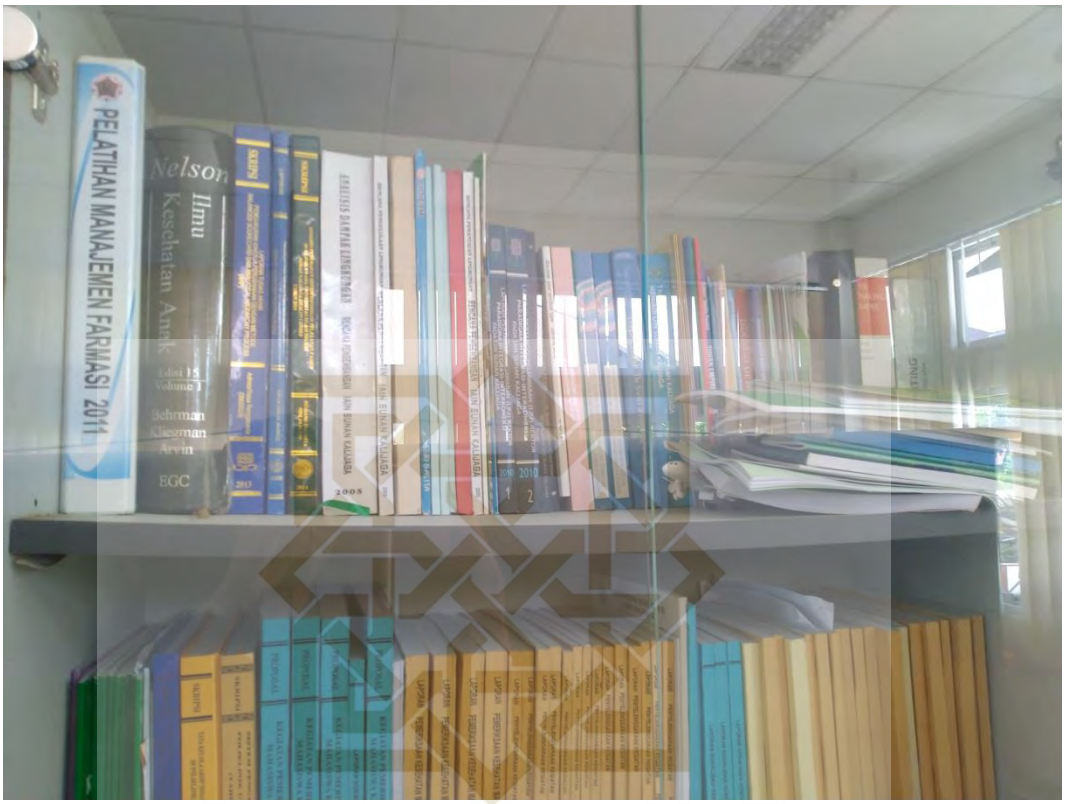


LAMPIRAN 15

Gambar Objek Tempat Audit (Ruang Tamu)

LAMPIRAN 16

Gambar Objek Tempat Audit (Ruang Aset dan Informasi)



LAMPIRAN 17

Gambar Objek Tempat Audit (Pantri)

LAMPIRAN 18

Gambar Objek Tempat Audit (Laboratorium)

LAMPIRAN 19

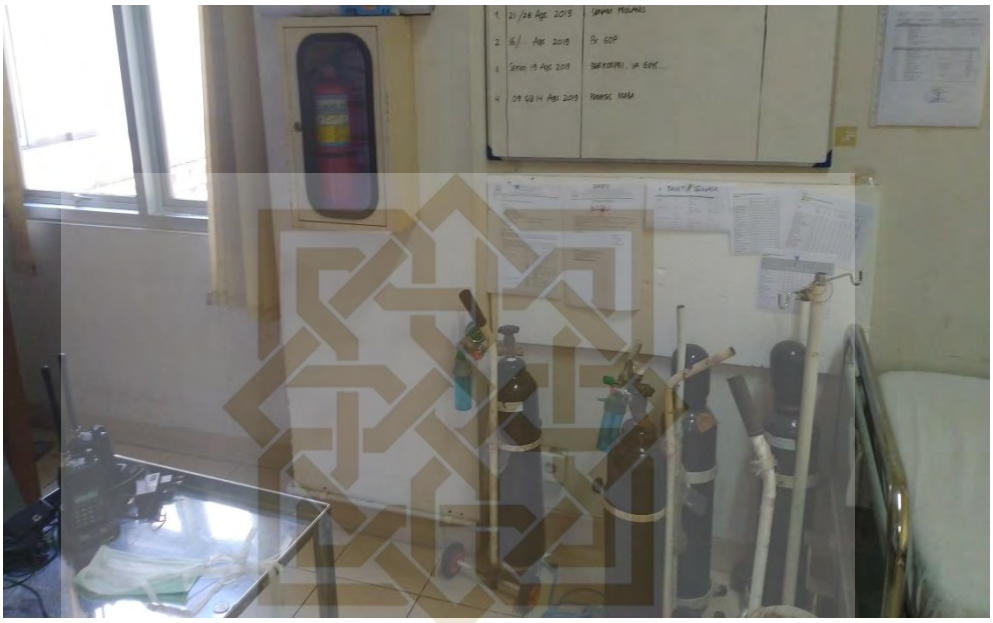
Gambar Objek Tempat Audit (Ruang Apotek)

LAMPIRAN 20

Gambar Objek Tempat Audit (Tempat Rekam Medis)

LAMPIRAN 21

Gambar Objek Tempat Audit (Penempatan Barang Berbahaya dan Pencegahnya)



LAMPIRAN 22

Gambar Objek Tempat Audit Tambahan

(*Fingerprint*)

(*Switch/Router*)

(Parkir)

(Alat Tulis Kantor (ATK))

BIODATA

Nama	: Ferdian Noor Pambudi
Tempat, Tanggal Lahir	: Bandar Lampung, 10 Januari 1994
Jenis Kelamin	: Laki-laki
Golongan Darah	: O
Agama	: Islam
Kewarganegaraan	: Indonesia
Nama Ayah	: Drs.Budiyono
Nama Ibu	: Dra.Ismulyani
Alamat Rumah	: Desa Puri Rt.04 Rw.04 Kec. Pati, Kab. Pati, Jawa Tengah 59113
Alamat Yogyakarta	: Jl. Bimo Kurdo No.64f, Papringan, Caturtunggal, Rt.019 Rw.001 Kec. Depok, Kab. Sleman, Daerah Istimewa Yogyakarta 55281
No. HP	: 085743875932
E-mail	: ferdiannoorpambudi@gmail.com
Riwayat Pendidikan	
2000-2003	: SD Negeri 2 Palapa Bandar Lampung
2003-2006	: SD Puri 02 Pati
2006-2009	: SMP Negeri 5 Pati
2009-2012	: SMA PGRI 1 Pati
2012-2019	: S1 Teknik Informatika, Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta