ANALISIS KINERJA *ROUTING PROTOCOL* BGP DAN EIGRP TERHADAP SERANGAN *PACKET SNIFFING* DAN *SPOOFING* BERBASIS GNS3

SKRIPSI

ESMERALDA WANGSA
1907423001

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2023

ANALISIS KINERJA *ROUTING PROTOCOL* BGP DAN EIGRP TERHADAP SERANGAN *PACKET SNIFFING* DAN *SPOOFING* BERBASIS GNS3

SKRIPSI

Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan untuk Memperoleh Diploma Empat Politeknik

Esmeralda Wangsa

1907423001

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2023

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini :

Nama	: Esmeralda Wangsa
NIM	: 1907423001
Jurusan/ProgramStudi	: T.Informatika dan Komputer / Teknik Multimedia dan Jaringan
Judul skripsi	: Analisis Kinerja *Routing Protocol* BGP Dan EIGRP Terhadap Serangan *Packet Sniffing* Dan *Spoofing* Berbasis GNS3

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, 21 Juli 2023

Yang membuat pernyataan

Esmeralda Wangsa

NIM.1907423001

LEMBAR PENGESAHAN

Skripsi diajukan oleh :

Nama	: Esmeralda Wangsa
NIM	: 1907423001
Jurusan/ProgramStudi	: T.Informatika dan Komputer / Teknik Multimedia dan Jaringan
Judul skripsi	: Analisis Kinerja *Routing Protocol* BGP Dan EIGRP Terhadap Serangan *Packet Sniffing* Dan *Spoofing* Berbasis GNS3

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari ..Selasa....., Tanggal.....1....., Bulan...Agustus....., Tahun....2023..... dan dinyatakan **LULUS**.

Disahkan oleh

Pembimbing I	: Ayu Rosyida Zain, S.ST., M.T	( )
Penguji I	: Maria Agustin, S.Kom., M.Kom	( )
Penguji II	: Indra Hermawan, S.kom., M.Kom	( )
Penguji III	: Ariawan Andi Suhandana, S.Kom., M.T.I	( )

Mengetahui :
Ketua Jurusan Teknik Informatika dan Komputer

Dr. Anita Hidayati, S.Kom., M.Kom.
NIP.197908032003122003

KATA PENGANTAR

Puji dan syukur kehadirat Tuhan Yang Maha Esa yang telah memberikan rahmat dan karunia-Nya kepada penulis, karena atas berkat dan rahmatnya penulis berhasil menyelesaikan laporan skripsi ini tepat pada waktunya sehingga penulis dapat menyelesaikan skripsi ini dengan judul Analisis Kinerja *Routing Protocol* BGP Dan EIGRP Terhadap Serangan *Packet Sniffing* Dan *Spoofing* Berbasis GNS3. Tujuan dari dilakukan penulisan laporan ini sebagai rangka untuk memenuhi salah satu syarat untuk mencapai gelar Diploma Empat Politeknik. Dalam penyusunan laporan ini, penulis sadar bahwa selesainya laporan skripsi ini berkat dukungan dan bimbingan dari berbagai pihak. Oleh karena itu penulis mengucapkan terima kasih kepada :

1. Tuhan Yang Maha Esa yang selalu memberikan hikmat dan rahmatnya dalam menyelesaikan Tugas Akhir
2. Orang tua dan keluarga serta sahabat penulis yang telah memberikan bantuan dukungan moral dan material.
3. Ibu Ayu Rosyida Zain, S.ST., M.T. selaku dosen pembimbing yang mengarahkan dalam penelitian ini.
4. Rekan seperjuangan program studi Teknik Multimedia dan Jaringan yang telah membantu, mendukung dan menemani hingga selesainya penelitian.
5. Seluruh jajaran Dosen dan Staf Teknik Informatika dan Komputer Politeknik Negeri Jakarta

Akhir kata, penulis berharap Tuhan Yang Maha Esa membalas segala bentuk kebaikan dari semua pihak yang telah membantu. Semoga laporan skripsi ini dapat bermanfaat bagi pembaca dan untuk pengembangan ilmu.

Depok, 21 Juli 2023

Esmeralda Wangsa

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI

SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan dibawah ini :

Nama	: Esmeralda Wangsa
NIM	: 1907423001
Jurusan/ProgramStudi	: T.Informatika dan Komputer / Teknik Multimedia dan Jaringan

Demi pengembangan ilmu pengetahuan , menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul :

ANALISIS KINERJA *ROUTING PROTOCOL* BGP DAN EIGRP TERHADAP SERANGAN *PACKET SNIFFING* DAN *SPOOFING* BERBASIS GNS3

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalihmediakan/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta..

Demikian pernyatan ini saya buat dengan sebenarnya.

Depok, 21 Juli 2023

Yang membuat pernyataan

Esmeralda Wangsa

NIM.1907423001

Analisis Kinerja Terhadap *Routing Protocol* BGP Dan EIGRP Untuk Serangan *Packet Sniffing* Dan *Spoofing* Berbasis GNS3

Abstrak

Keamanan jaringan yang kuat sangat penting bagi organisasi atau individu yang bergantung pada infrastruktur jaringan karena jika gagal dalam pengamanan dapat membuat jaringan terkena serangan. *Routing protocol* yang tidak aman atau rentan terhadap serangan dapat menyebabkan ketidakstabilan jaringan seperti serangan *spoofing* dan *sniffing* yang dapat menyebabkan paket data diarahkan ke jalur yang salah atau terhenti, mengakibatkan gangguan jaringan. Peretas dapat menciptakan peluang untuk menyerang dan merusak jaringan yang dibangun. Permasalahannya adalah bagaimana kinerja suatu jaringan yang menggunakan BGP dan EIGRP dalam menggunakan serangan *sniffing* dan *spoofing* dan pengamanan berbasis *firewall* dengan simulasi GNS3. Tujuan dari penelitian ini adalah untuk menganalisis performa dari BGP dan EIGRP dengan serangan *sniffing* dan *spoofing* menggunakan simulasi GNS3 berdasarkan parameter *packet loss*, *jitter*, *throughput* dan *delay*. Analisis kinerja protokol BGP dan EIGRP diperlukan untuk memahami dampak terhadap serangan dan metode pengamanan yang diterapkan. Metode pengamanan yang digunakan pada penelitian ini adalah pemisahan VLAN dan pemasangan *firewall*. Parameter yang digunakan pada penelitian ini adalah *packet loss*, *jitter*,dan *delay*. Protokol EIGRP dengan serangan *spoofing* dan *sniffing* memiliki nilai *packet loss* lebih rendah sebesar 6.16% dibandingkan BGP . Protokol BGP dengan serangan *spoofing* dan *sniffing* memiliki nilai *jitter* lebih rendah sebesar 61.26 ms dan *delay* lebih rendah sebesar 44.31 ms dibandingkan EIGRP. Hasil penelitian menunjukkan protokol BGP terbukti lebih unggul dibandingkan protokol EIGRP dalam berbagai kondisi uji. Meskipun protokol EIGRP menunjukkan keunggulan dalam beberapa aspek pada beberapa kondisi uji tertentu, namun secara keseluruhan, protokol BGP dapat dianggap lebih unggul dalam situasi yang lebih umum yang diuji.

Kata kunci: *packet sniffing*, *spoofing*, BGP, EIGRP

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar belakang

Keamanan jaringan yang kuat sangat penting bagi organisasi atau individu yang bergantung pada infrastruktur jaringan karena jika gagal dalam pengamanan dapat membuat jaringan terkena serangan. *Routing protocol* yang tidak aman atau rentan terhadap serangan dapat menyebabkan ketidakstabilan jaringan seperti serangan *spoofing* yang dapat menyebabkan paket data diarahkan ke jalur yang salah atau terhenti, mengakibatkan gangguan jaringan. Keamanan pada *routing protocol* yang baik dapat membantu mencegah serangan terhadap jaringan, seperti serangan *spoofing*, *sniffing*, dan lainnya. Hal ini berdampak pada stabilitas dan ketersediaan jaringan secara keseluruhan. Semakin hari serangan semakin meningkat, hal ini didukung oleh laporan Kaspersky yang menyatakan bahwa aktivitas jaringan yang mencurigakan mencapai 22%. Salah satunya adalah adanya serangan spoofing(Hafizh, Riadi and Fadlil, 2020). *Spoofing* adalah teknik serangan yang cara kerjanya dengan penyerang menyamar sebagai sumber terpercaya atau resmi untuk memperoleh akses yang tidak sah. Selain *spoofing*, terdapat serangan metode *packet sniffing*. *Packet sniffing* menyediakan konfigurasi antarmuka jaringan untuk menampilkan semua informasi ditransmisikan melalui jaringan(Albadri, 2020). *Packet sniffer* juga dapat digunakan oleh peretas untuk menangkap informasi jaringan yang sensitif seperti kata sandi dan informasi akun, dan lain lain(Mphil and Saranya, 2018). *Attacker* yang digunakan yaitu Ettercap dengan memanfaatkan service ARP (*Address Resolution Protocol*) *poisoning*. ARP (*Address Resolution Protocol*) *poisoning* adalah serangan di mana penyerang *poisoning* cache ARP target host dan menempatkan dirinya di antara lalu lintas sah yang mengarah ke serangan seperti MITM (*Man in the Middle Attack), sniffing, connection hijacking, connection spoofing* dan DoS *(Denial of Service)*(Alam, 2018). Ettercap menganalisis serangan ARP *poisoning* dengan memeriksa paket dari sumber ke tujuan dan korban ARP *poisoning*(Majidha and Santhiyakumari, 2021). *Operator data center* umumnya

menggunakan BGP untuk perutean dan BGP telah membuat terobosan ke *data center* karena skalabilitasnya, kontrol kebijakan yang ekstensif, dan rekam jejak yang terbukti dalam menjalankan internet selama beberapa dekade(Abhashkumar *et al.*, 2021). *Border Gateway Protocol* (BGP) sebagai protokol perutean standar yang menghubungkan internet untuk membawa data ke seluruh dunia rentan terhadap serangan spoofing(Banu.A and Ganapthi, 2021). EIGRP memiliki waktu konvergensi yang cepat dan dapat dengan cepat beradaptasi dengan perubahan di jaringan dan memperbarui tabel perutean(Prehanto, Indriyanti and Permadi, 2021). EIGRP dapat diskalakan dan dapat mendukung jaringan besar dengan banyak router(Hossain *et al.*, 2020). EIGRP adalah pilihan terbaik untuk jaringan besar dan kecil karena memiliki konvergensi tercepat dan EIGRP menggunakan *bandwidth* secara efisien(Hossain *et al.*, 2020). Serangan *spoofing* dan *sniffing* dapat menyebabkan gangguan serius pada kinerja jaringan, menyebabkan peningkatan *packet loss*, dan meningkatkan *jitter* serta *delay* dalam pengiriman data. Selain itu, serangan-serangan ini juga dapat mengancam keamanan data dan informasi sensitif yang dikirimkan melalui jaringan. Mengidentifikasi dan mengatasi ancaman ini dengan mengimplementasikan mekanisme keamanan seperti performa jaringan dan pengamanan menjadi suatu keharusan untuk memastikan kinerja jaringan yang optimal dan melindungi data dari potensi kebocoran atau manipulasi yang merugikan. Dengan meningkatkan kesadaran akan pengaruh serangan *spoofing* dan *sniffing* terhadap kinerja jaringan, organisasi dan pengelola jaringan dapat mengambil langkah-langkah proaktif untuk meningkatkan keamanan dan kinerja jaringan mereka.

Serangan *Packet Sniffing* terhadap *Routing Protocol* RIPv2, OSPF, dan EIGRP pernah dibuat peneliti sebelumnya yaitu Sigit Widodo (Widodo, 2021). Penelitian tersebut dirancang 2 model topologi dengan 6 skenario dan 4 parameter *Quality of Service* menggunakan *routing protocol* yang digunakan yaitu RIPv2, OSPF, dan EIGRP serta menggunakan GNS3. Hasil penelitian menunjukkan *routing protocol* EIGRP skenario normal memiliki keunggulan di parameter *throughput* dan *jitter*, *routing protocol* RIPv2 skenario normal memiliki keunggulan di parameter *packet loss* dan *latency*, *dan routing protocol* RIPv2, OSPF, dan EIGRP dengan serangan

packet sniffing selalu bernilai lebih buruk dibandingkan *routing protocol normal*. Pada penelitian tersebut tidak menggunakan *routing protocol* BGP. Deteksi dan Mitigasi Spoofing Border Gateway Protocol pernah dibuat peneliti sebelumnya yaitu (Banu.A and Ganapthi, 2021) dengan menggunakan Algoritma Hybrid Bat Optimization dan Kriptografi. Pada penelitian tersebut tidak menggunakan metode serangan *packet sniffing.*

Penulis melakukan pengembangan dari kedua penelitian tersebut. Penelitian ini membahas tentang deteksi dan pengamanan dari serangan *Packet Sniffing* dan *Spoofing* terhadap *Routing Protocol* BGP dan EIGRP menggunakan GNS3 untuk pengembangan penelitian sebelumnya. Metode serangan yang digunakan pada penelitian ini adalah *Packet Sniffing* dan *Spoofing* terhadap *Routing Protocol* BGP dan EIGRP menggunakan aplikasi Wireshark dan Ettercap. Pengamanan dari serangan *packet sniffing* dan *spoofing* terhadap *Routing Protocol* BGP dan EIGRP adalah dengan pemisahan VLAN,pemasangan *firewall* dan enkripsi *web server* (HTTPS). Parameter dalam penelitian ini adalah *packet loss, jitter, throughput* dan *delay*.

1.2 Perumusan Masalah

Rumusan masalah dalam penelitian ini adalah: Bagaimana melihat kinerja *routing protocol* BGP dan EIGRP terhadap serangan *packet sniffing* dan *spoofing* berdasarkan *packet loss, jitter, throughput* dan *delay?*.

1.3 Batasan Masalah

Batasan masalah yang ditentukan dalam pengamanan dari serangan *packet sniffing* dan *spoofing* terhadap *routing protocol* BGP menggunakan GNS3 adalah sebagai berikut:

1. Penelitian ini menggunakan metode simulasi jaringan dengan aplikasi GNS3 versi 2.2.40.
2. *Routing protocol* yang digunakan adalah BGP dan EIGRP.
3. Penelitian ini menggunakan dua metode serangan yaitu *packet sniffing* dan *spoofing*. Tools yang digunakan untuk serangan *packet sniffing* dan *spoofing* adalah ettercap dan wireshark.

4. *Client* diserang oleh *attacker* dalam jaringan yang sama.
5. Penelitian ini menggunakan metode pengamanan dengan pemisahan VLAN,pemasangan *firewall* dan enkripsi *web server* (HTTPS).
6. Penelitian ini menggunakan parameter *packet loss*, *jitter*, *throughput* dan *delay*.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Tujuan dari penelitian ini adalah untuk menganalisis performa dari BGP dan EIGRP dengan serangan *sniffing* dan *spoofing* menggunakan simulasi GNS3 berdasarkan parameter *packet loss*, *jitter*, *throughput* dan *delay*.

1.4.2 Manfaat

Hasil penelitian ini dapat bermanfaat untuk mengetahui protokol routing BGP atau EIGRP yang lebih baik sehingga ketahanan serangan lebih tinggi dan kinerja lebih stabil.

1.5 Sistematika Penulisan

Berikut adalah sistematika penulisan yang digunakan dalam penelitian ini, yaitu sebagai berikut:

1. Bab I Pendahuluan

   Bab I merupakan pendahuluan yang membahas tentang latar belakang dari penelitian, rumusan masalah, batasan masalah, tujuan dan manfaat dari penelitian, dan sistematika penulisan penelitian ini.
2. Bab II Tinjauan Pustaka

   Bab II merupakan tinjauan pustaka yang berisi tentang landasan-landasan teori pada penelitian ini dan penelitian-penelitian terdahulu yang sejenis.
3. Bab III Metode Penelitian

   Bab III merupakan metode penelitian yang berisi tentang rancangan penelitian, tahapan penelitian, dan objek penelitian.
4. Bab IV Pembahasan

Bab IV merupakan pembahasan yang berisi analisis kebutuhan, perancangan sistem, implementasi sistem, pengujian, deskripsi pengujian, prosedur pengujian, data hasil pengujian, dan analisis data atau evaluasi.

5. Bab V Penutup

   Bab V merupakan penutup yang berisi kesimpulan dan saran.

BAB V

PENUTUP

5.1 Kesimpulan

Kesimpulan dari penelitian dengan 8 skenario, protokol BGP lebih unggul daripada protokol EIGRP. Akan tetapi, protokol EIGRP lebih unggul dalam 2 kondisi yaitu *packet loss* dengan gabungan serangan spoofing dan sniffing dan jitter dengan pengamanan. Berdasarkan jumlah keseluruhan nilai rata-rata dari 8 skenario dengan indeks parameter QoS standarisasi dari TIPHON, protokol BGP memiliki nilai rata-rata sebesar 2.88 dan dikategorikan sebagai 'Sedang', sementara protokol EIGRP memiliki nilai rata-rata sebesar 2.75 dan juga dikategorikan sebagai 'Sedang'. Dalam hal nilai rata-rata sesusi standarisasi TIPHON, protokol BGP memiliki keunggulan sebesar 0.13 poin dibandingkan dengan protokol EIGRP.

5.2 Saran

Sebagai arah penelitian selanjutnya, disarankan untuk menjelajahi variasi protokol routing yang lain, bersama dengan pendekatan baru dalam hal serangan dan keamanan jaringan. Selain itu, menggali metode baru untuk menghadapi ancaman siber yang terus berkembang akan membantu mengantisipasi tantangan keamanan di masa depan. Mengintegrasikan strategi perlindungan yang inovatif dan adaptif dalam lingkungan jaringan dapat memberikan pandangan yang lebih kaya tentang upaya perlindungan data dan infrastruktur secara menyeluruh.

DAFTAR PUSTAKA

Abhashkumar, A. *et al.* (2021) 'Running BGP in data centers at scale', *Proceedings of the 18th USENIX Symposium on Networked Systems Design and Implementation, NSDI 2021*, pp. 65–80.

Ahutu, O.R. and El-Ocla, H. (2020) 'Centralized Routing Protocol for Detecting Wormhole Attacks in Wireless Sensor Networks', *IEEE Access*, 8, pp. 63270–63282. doi:10.1109/ACCESS.2020.2983438.

Alam, M. (2018) 'Investigating ARP poisoning', (May). doi:10.6084/m9.figshare.14706240.

Albadri, R.F. (2020) 'Development of a network packet sniffing tool for internet protocol generations', *International Journal of Cloud Computing*, 9(2–3), pp. 232–244. doi:10.1504/IJCC.2020.109378.

Albar, R. and Putra, R.O. (2022) 'Sniffing Dan Implementasi Keamanan Jaringan Network Security Analysis Using the Method Sniffing and Implementation of Network Security on Microtik Router Os V6 . 48 . 3 Using Port Knocking Method', *Journal of Informatics and Computer Science*, 8(1), pp. 1–11.

Aprianto Budiman, M. Ficky Duskarnaen and Hamidillah Ajie (2020) 'Analisis Quality of Service (Qos) Pada Jaringan Internet Smk Negeri 7 Jakarta', *PINTER : Jurnal Pendidikan Teknik Informatika dan Komputer*, 4(2), pp. 32–36. doi:10.21009/pinter.4.2.6.

Apriza, U.D. *et al.* (2020) 'Analisis Qos (Quality of Service) Pada Layanan Internet Jaringan Biznet Home Kota Pontianak', *Digital*, pp. 0–30. Available at: https://jurnal.untan.ac.id/index.php/jteuntan/article/view/57249/75676594205.

Ayesha Nasir and Unsa Tariq (2018) 'A Comparative Study of Routing Protocols Including RIP, OSPF and BGP', *Lahore Garrison University Research Journal of Computer Science and Information Technology*, 2(2), pp. 47–56. doi:10.54692/lgurjcsit.2018.020236.

Banu.A, S. and Ganapthi, P. (2021) 'Detection and Mitigation of Border Gateway Protocol Spoofing Using Hybrid Bat Optimization Algorithm and Cryptography', *SSRN Electronic Journal*, 2019(ICICNIS), pp. 391–411. doi:10.2139/ssrn.3769224.

Cv, R.K. and Goyal, H. (2019) 'IPv4 to IPv6 Migration and Performance Analysis using GNS3 and Wireshark', *Proceedings - International Conference on Vision Towards Emerging Trends in Communication and Networking, ViTECoN 2019*, pp. 1–6. doi:10.1109/ViTECoN.2019.8899746.

ETSI (2020) 'Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); General aspects of Quality of Service (QoS)', *Etsi Tr 101 329 V2.1.1*, 1, pp. 1–37.

Fachri, A., Neforawati, I. and Kurniawan Program Studi Teknik Multimedia dan Jaringan Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta Jl

ProfDRGA Siwabesy, A. (2021) 'Optimalisasi Server Proxmox pada NICT UIN Syarif Hidayatullah Jakarta', *Optimalisasi Server Proxmox pada NICT UIN Syarif Hidayatullah Jakarta JURNAL MULTINETICS*, 7(2), pp. 196–203.

Fiade, A., Agustian, M.A. and Masruroh, S.U. (2019) 'Analysis of Failover Link System Performance in OSPF, EIGRP, RIPV2 Routing Protocol with BGP', *2019 7th International Conference on Cyber and IT Service Management, CITSM 2019* [Preprint]. doi:10.1109/CITSM47753.2019.8965373.

Hafizh, M.N., Riadi, I. and Fadlil, A. (2020) 'Forensik Jaringan Terhadap Serangan ARP Spoofing menggunakan Metode Live Forensic', *Jurnal Telekomunikasi dan Komputer*, 10(2), p. 111. doi:10.22441/incomtech.v10i2.8757.

Hossain, M.A. *et al.* (2020) 'Performance Comparison of EIGRP, OSPF and RIP Routing Protocols using Cisco Packet Tracer and OPNET Simulator', *Global Journal of Computer Science and Technology*, 20(2), pp. 1–7. doi:10.34257/gjcstgvol20is2pg1.

Ibrahim, M. (2023) 'Implementasi dan Analisis Profil Sistem Pada Virtualisasi Fortigate Firewall Berdasarkan Metrik Sumber Daya Komputasi Implementation and Analysis of System Profile on Fortigate Firewall Virtualization Based on Computing Resource Metrics', 10(2), pp. 1505–1511.

Ilham Firdaus, Januar Al Amien and Soni, S. (2020) 'String Matching untuk Mendeteksi Serangan Sniffing (ARP Spoofing) pada IDS Snort', *Jurnal CoSciTech (Computer Science and Information Technology)*, 1(2), pp. 44–49. doi:10.37859/coscitech.v1i2.2180.

Ismail, H., Germanus, D. and Suri, N. (2017) 'P2P routing table poisoning: A quorum-based sanitizing approach', *Computers and Security*, 65, pp. 283–299. doi:10.1016/j.cose.2016.12.007.

Kalra, H. and Singh, Abhishek Pratap Sadhya, D. (2021) 'Anomaly detection in Border Gateway Protocol using supervised machine learning', *IEEE Bombay Section Signature Conference (IBSSC)* [Preprint]. doi:10.1109/IBSSC53889.2021.9673281.

Korniyenko, B., Galata, L. and Ladieva, L. (2019) 'Research of Information Protection System of Corporate Network Based on GNS3', *2019 IEEE International Conference on Advanced Trends in Information Theory, ATIT 2019 - Proceedings*, pp. 244–248. doi:10.1109/ATIT49449.2019.9030472.

Kumar, S., Jigyasu, S. and Singh, V. (2021) 'Network Traffic Monitor and Analysis Using Packet Sniffer', 9(7), pp. 77–82.

Kurniawan, K. and Prihanto, A. (2022) 'Analisis Quality Of Service (QoS) Pada Routing Protocol Routing OSPF (Open Short Path First)', *Journal of Informatics and Computer Science (JINACS)*, 3(03), pp. 358–365. doi:10.26740/jinacs.v3n03.p358-365.

Luthfansa, Z.M. and Rosiani, U.D. (2021) 'Pemanfaatan Wireshark untuk Sniffing Komunikasi Data Berprotokol HTTP pada Jaringan Internet', *Journal of Information Engineering and Educational Technology*, 5(1), pp. 34–39.

doi:10.26740/jieet.v5n1.p34-39.

M, M.F.K. and Santhiyakumari, N. (2021) 'A Survey On Network Packet Inspection And ARP2021.pdf', pp. 1136–1141.

Mahmood, A.N. (2020) 'Performance Analysis of Routing Protocols RIP, EIGRP, OSPF and IGRP using Networks connector'. doi:10.4108/eai.28-6-2020.2298167.

Martias, M., Azhari, A. and Saputra, D. (2020) 'Penerapan Jaringan Virtual Local Area Network Dengan Cisco Packet Tracer', *INSANTEK - Jurnal Inovasi dan Sains Teknik Elektro*, 1(1), pp. 28–33. Available at: http://ejournal.bsi.ac.id/ejurnal/index.php/insantek28.

Moudni, H. *et al.* (2016) 'Performance analysis of AODV routing protocol in MANET under the influence of routing attacks', *Proceedings of 2016 International Conference on Electrical and Information Technologies, ICEIT 2016*, pp. 536–542. doi:10.1109/EITech.2016.7519658.

Mphil, R.K. and Saranya, S. (2018) 'Packet Sniffing : Monitoring and Analysis Using Sniffing Method', 5(11), pp. 202–206.

Musril, H.A. (2015) 'ANALISIS UNJUK KERJA RIPv2 DAN EIGRP DALAM DYNAMIC ROUTING PROTOCOL', *Jurnal Elektro dan Telekomunikasi Terapan*, 2(2), pp. 116–124. doi:10.25124/jett.v2i2.99.

Pingle, B., Mairaj, A. and Javaid, A.Y. (2018) 'Real-World Man-in-the-Middle (MITM) Attack Implementation Using Open Source Tools for Instructional Use', *IEEE International Conference on Electro Information Technology*, 2018-May, pp. 192–197. doi:10.1109/EIT.2018.8500082.

Pramana, M., Endang Setyati and F.X. Ferdinandus (2021) 'Identifikasi Serangan Denial Of Service (Dos) Di Jaringan Dengan Algoritma Decision Tree C4.5', *Wahana*, 73(2), pp. 13–29. doi:10.36456/wahana.v73i2.4071.

Prasetyo, I.B. (2019) 'Analisa Sniffing Paket ICMP menggunakan Wireshark', *Sistemasi*, 8(1), p. 221. doi:10.32520/stmsi.v8i1.339.

Prehanto, D.R., Indriyanti, A.D. and Permadi, G.S. (2021) 'Performance analysis routing protocol between RIPv2 and EIGRP with termination test on full mesh topology', *Indonesian Journal of Electrical Engineering and Computer Science*, 23(1), pp. 354–361. doi:10.11591/ijeecs.v23.i1.pp354-361.

Putu, I. *et al.* (2019) 'IMPLEMENTASI WIRESHARK DALAM MELAKUKAN PEMANTAUAN PROTOCOL JARINGAN (Studi Kasus : Intranet Jurusan Teknologi Informasi Universitas Udayana)', *Jurnal Mantik Penusa*, 3(1), p. 94.

Sadhu, P.K., Yanambaka, V.P. and Abdelgawad, A. (2022) 'Internet of Things: Security and Solutions Survey', *Sensors*, 22(19), pp. 1–51. doi:10.3390/s22197433.

Setiawan, A. and Rosyani, P. (2023) 'Analisis & Implementasi Kinerja Routing Protocol Is-Is (Intermediate System To Intermediate System)', 1(3), pp. 558–570.

Sudaryanto, S. *et al.* (2021) 'Web based Enhanced Interior Gateway Routing Protocol

(EIGRP) on cisco router 2811 using cisco's Application Programming Interface (API)', *Compiler*, 10(2), p. 79. doi:10.28989/compiler.v10i2.966.

Widianto, T.K. and Sulistyo, W. (2021) 'Implementasi Iptables Firewall dan Intrusion Detection System Untuk Mencegah Serangan DDoS Pada Linux Server', *MEANS (Media Informasi Analisa dan Sistem)*, 6(1), pp. 19–23. doi:10.54367/means.v6i1.1231.

Widodo, S. (2021) *Evaluasi Kinerja Routing Protocol Ripv2,Ospf, Dan Eigrp Terhadap Serangan Packet Sniffing*, *Fakultas Sains dan Teknologi UIN Syarif Hidayatullah Jakarta*. Available at: https://repository.uinjkt.ac.id/dspace/handle/123456789/56385.

Zainy, A. *et al.* (2023) 'Instalasi mikrotik pada virtualbox dan pengkoneksian antara mikrotikdi virtualbox dengan winbox di smk s teruna padang sidempuan', *Jurnal Adam*, 2(1), pp. 106–118.

DAFTAR RIWAYAT HIDUP

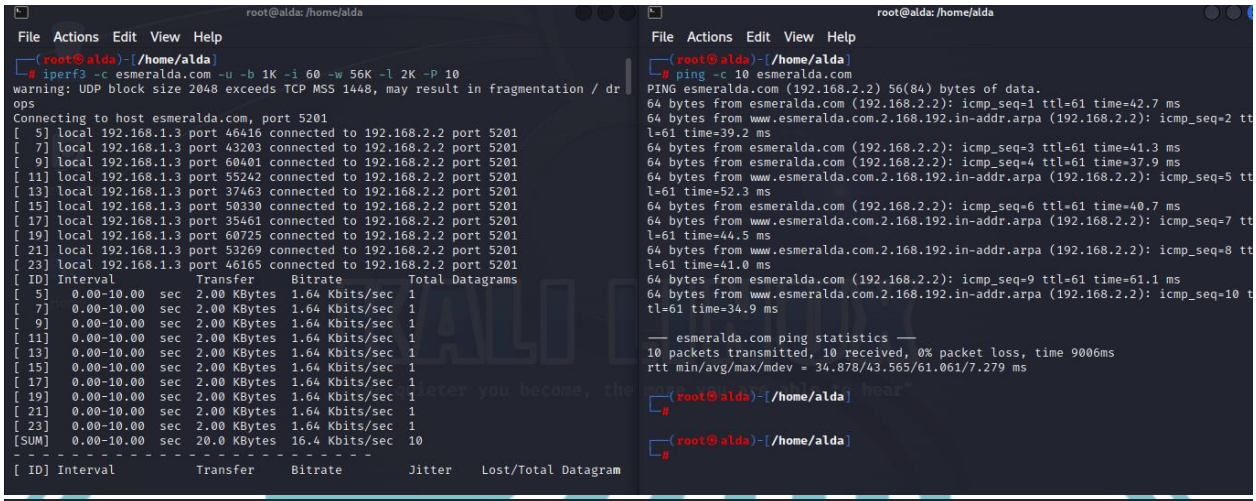
DAFTAR RIWAYAT HIDUP PENULIS

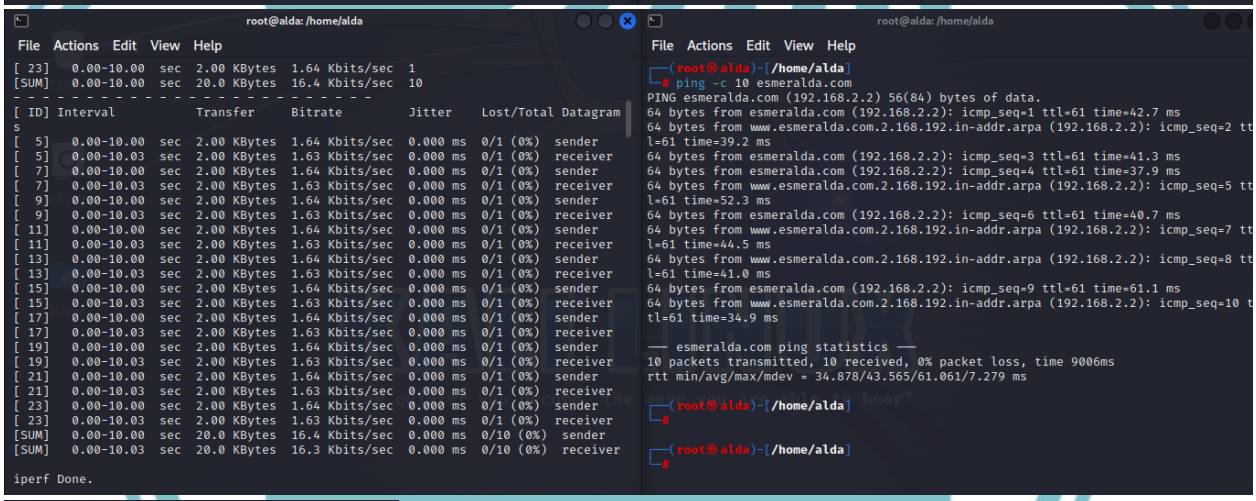
Lahir di Medan pada tanggal 8 Maret 2001.

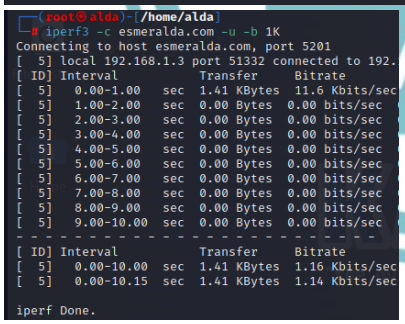
Riwayat pendidikan penulis adalah lulusan dari SD Pelita II, SMP Pelita II, dan SMKN 1 Jakarta. Pada tahun 2019 penulis melanjutkan pendidikan tinggi di kampus Politeknik Negeri Jakarta jurusan Teknik Informatika dan Komputer dengan Program Studi Teknik Multimedia dan Jaringan.

LAMPIRAN

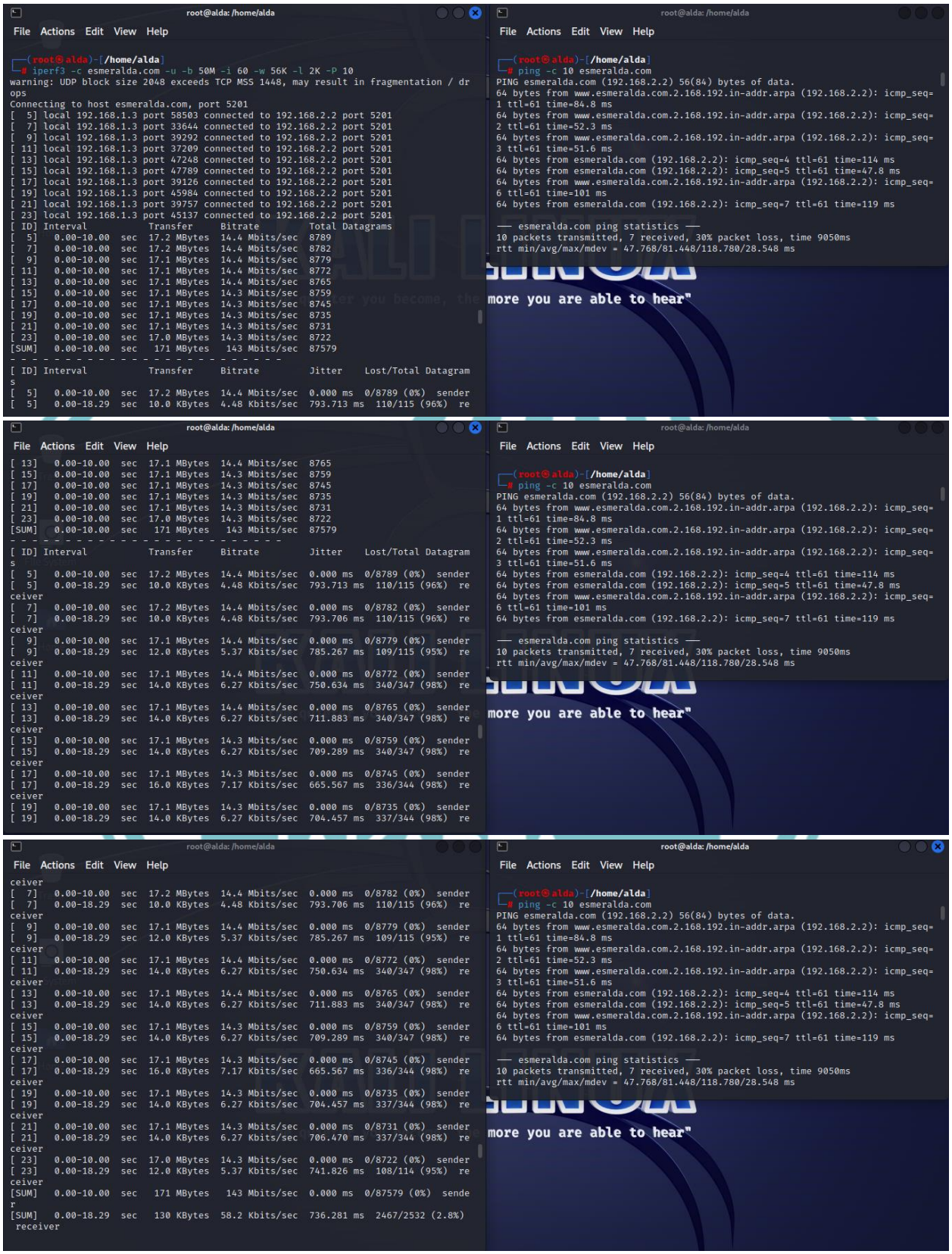
Screenshot hasil pengujian *spoofing* protokol BGP dengan *bandwidth* 1K.





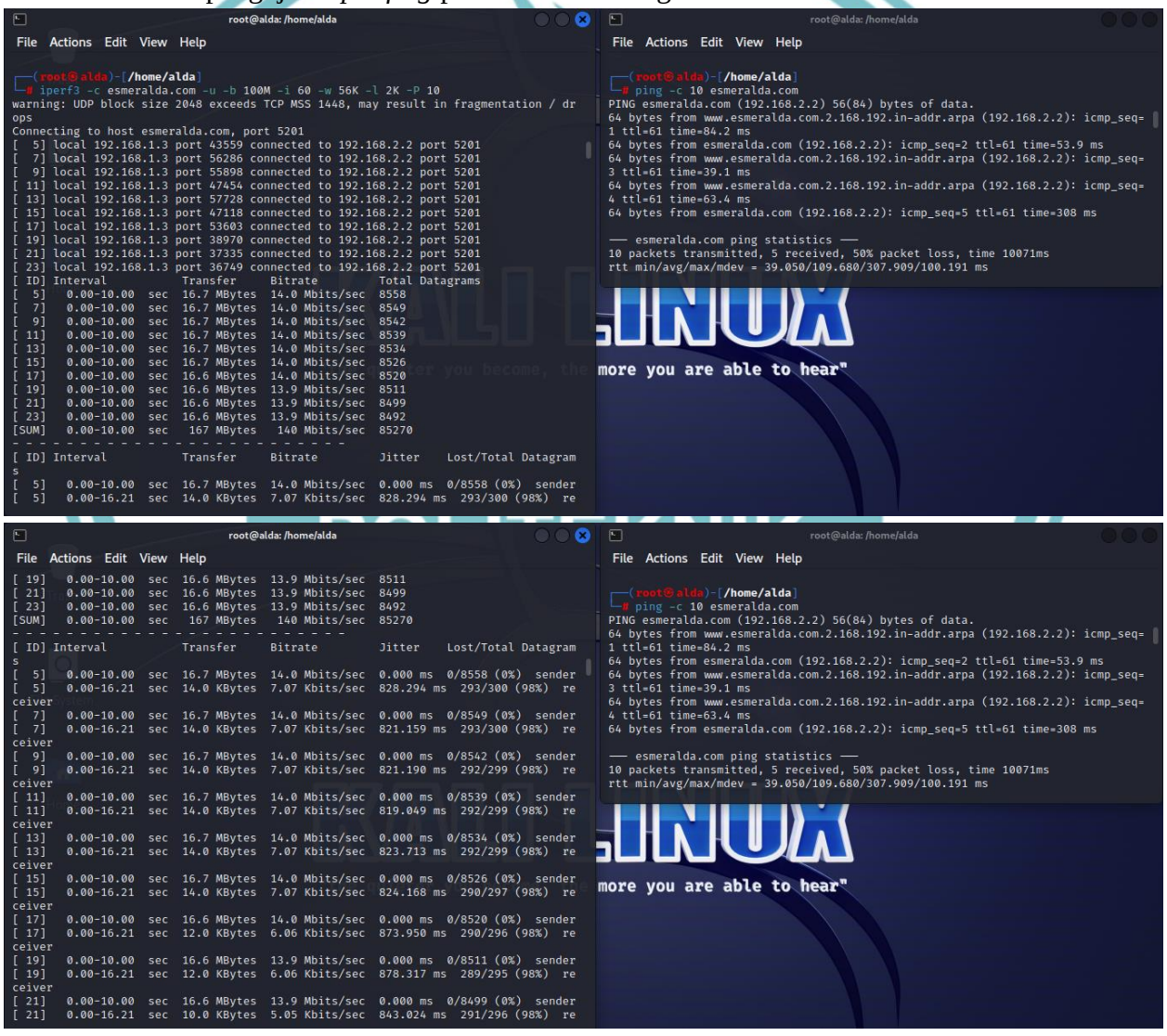


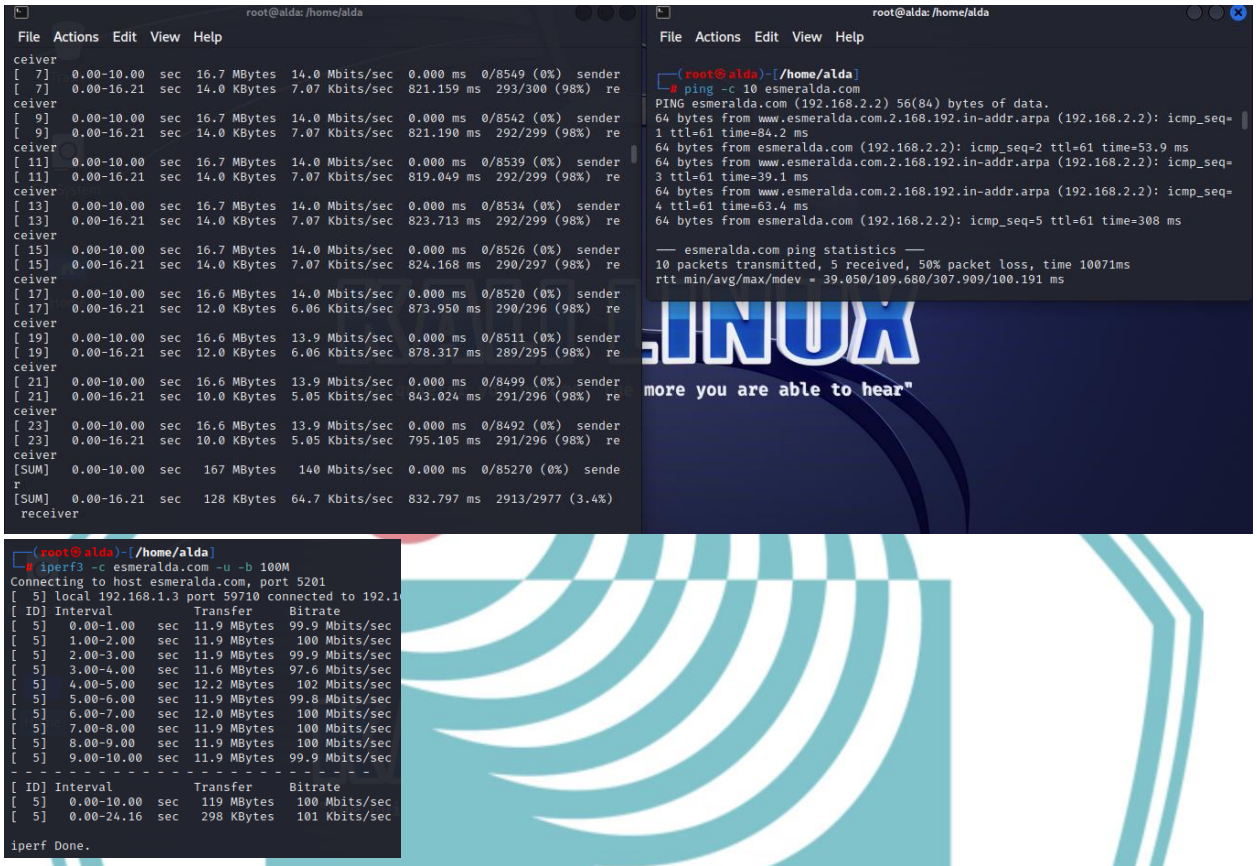
Screenshot hasil pengujian *spoofing* protokol BGP dengan *bandwidth* 50M.



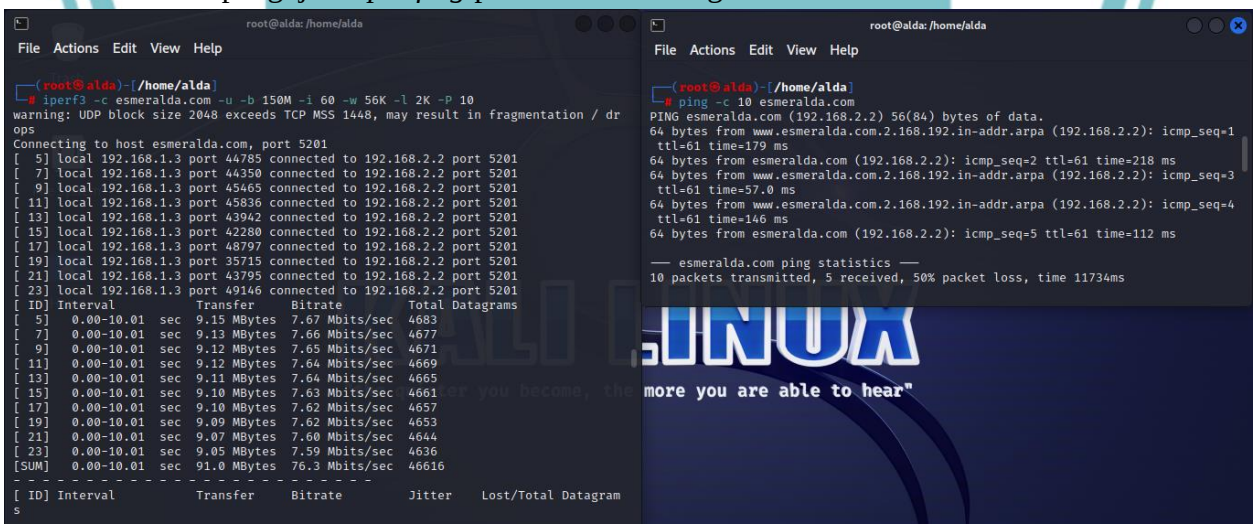
```
┌──(root㉿alda)-[/home/alda]
└─# iperf3 -c esmeralda.com -u -b 50M
Connecting to host esmeralda.com, port 5201
[  5] local 192.168.1.3 port 55537 connected to 192.16
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-1.00   sec  5.96 MBytes  49.9 Mbits/sec
[  5]   1.00-2.00   sec  5.96 MBytes  50.0 Mbits/sec
[  5]   2.00-3.00   sec  5.96 MBytes  50.0 Mbits/sec
[  5]   3.00-4.00   sec  5.88 MBytes  49.2 Mbits/sec
[  5]   4.00-5.00   sec  6.04 MBytes  50.7 Mbits/sec
[  5]   5.00-6.00   sec  5.96 MBytes  50.0 Mbits/sec
[  5]   6.00-7.00   sec  5.96 MBytes  50.0 Mbits/sec
[  5]   7.00-8.00   sec  5.94 MBytes  49.8 Mbits/sec
[  5]   8.00-9.00   sec  5.98 MBytes  50.2 Mbits/sec
[  5]   9.00-10.00  sec  5.96 MBytes  50.0 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-10.00  sec  59.6 MBytes  50.0 Mbits/sec
[  5]   0.00-18.80  sec   349 KBytes   152 Kbits/sec

iperf Done.
```

Screenshot hasil pengujian *spoofing* protokol BGP dengan *bandwidth* 100M.

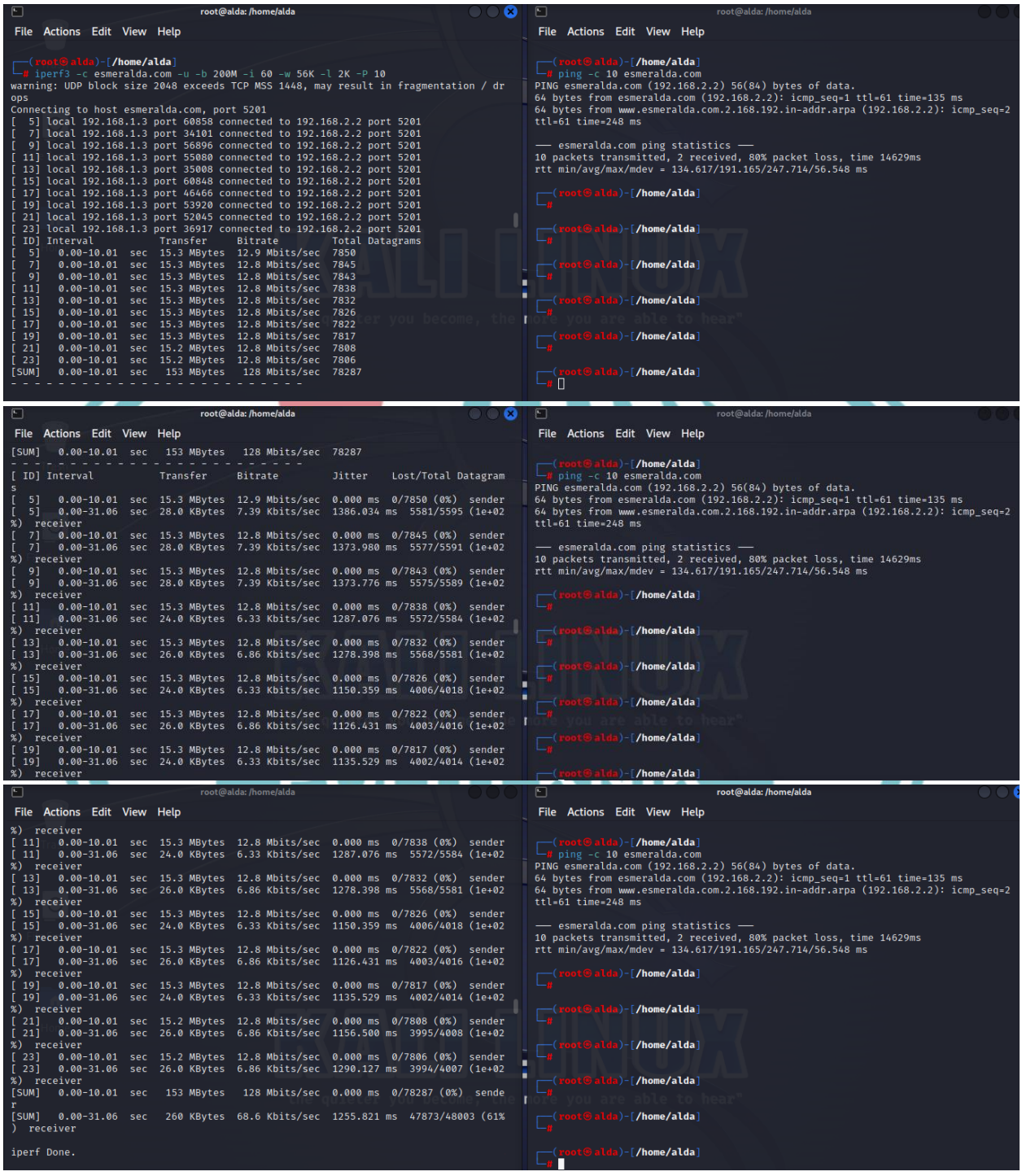




Screenshot hasil pengujian *spoofing* protokol BGP dengan *bandwidth* 150M.

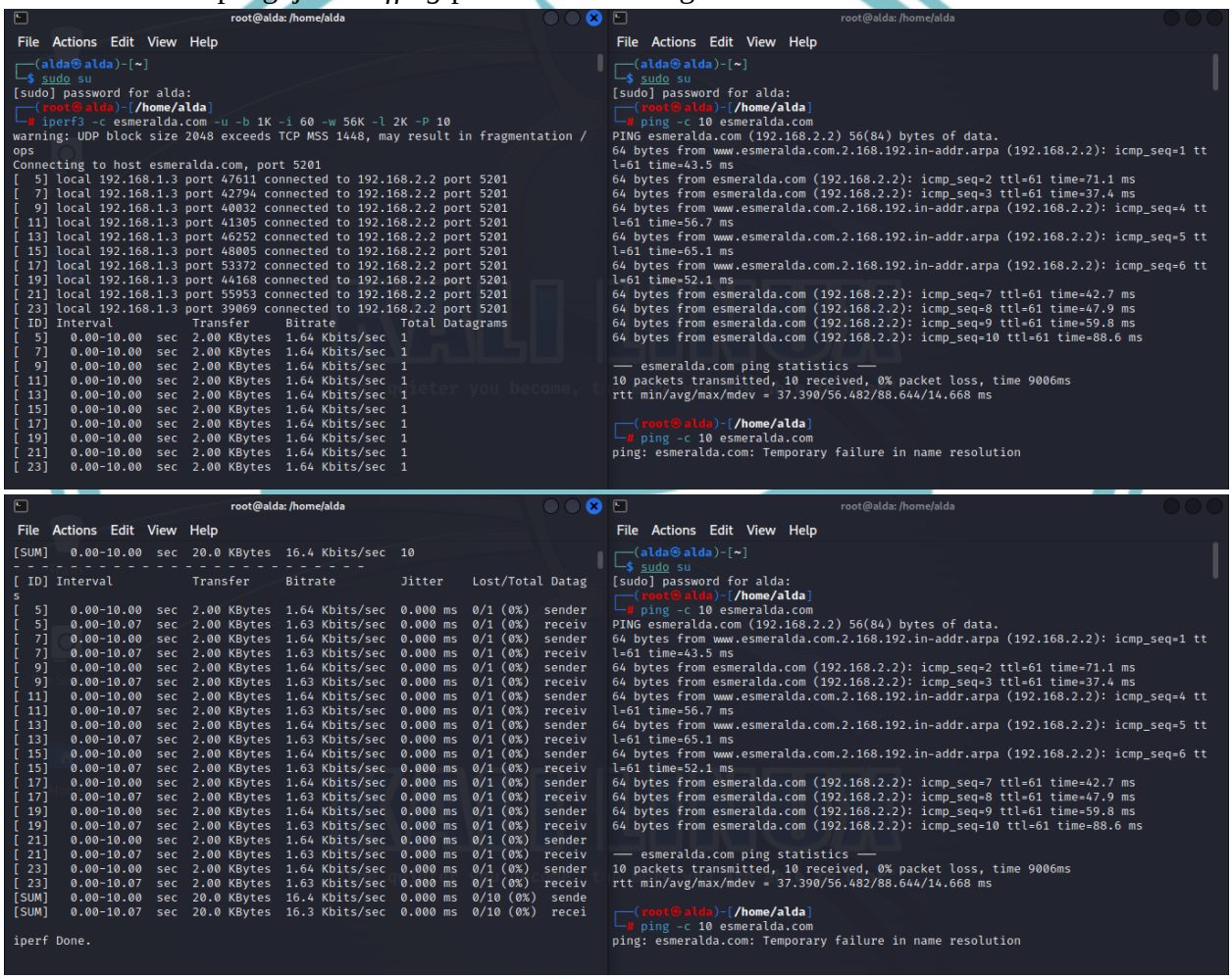


Screenshot hasil pengujian *spoofing* protokol BGP dengan *bandwidth* 200M.



```
┌──(root㉿alda)-[/home/alda]
└─# iperf3 -c esmeralda.com -u -b 200M
Connecting to host esmeralda.com, port 5201
[  5] local 192.168.1.3 port 47181 connected to 192.1
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-1.00   sec  14.9 MBytes   125 Mbits/sec
[  5]   1.00-2.00   sec  17.8 MBytes   149 Mbits/sec
[  5]   2.00-3.00   sec  16.5 MBytes   138 Mbits/sec
[  5]   3.00-4.00   sec  16.3 MBytes   137 Mbits/sec
[  5]   4.00-5.00   sec  17.2 MBytes   144 Mbits/sec
[  5]   5.00-6.00   sec  16.6 MBytes   138 Mbits/sec
[  5]   6.00-7.01   sec  17.5 MBytes   146 Mbits/sec
[  5]   7.01-8.00   sec  16.7 MBytes   141 Mbits/sec
[  5]   8.00-9.00   sec  16.8 MBytes   141 Mbits/sec
[  5]   9.00-10.00  sec  15.5 MBytes   130 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-10.00  sec   166 MBytes   139 Mbits/sec
[  5]   0.00-13.34  sec   164 KBytes   101 Kbits/sec

iperf Done.
```

Screenshot hasil pengujian *sniffing* protokol BGP dengan *bandwidth* 1K.



```
┌──(root㉿alda)-[/home/alda]
└─# iperf3 -c esmeralda.com -u -b 1K
Connecting to host esmeralda.com, port 5201
[  5] local 192.168.1.3 port 36392 connected to 192.
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-1.00   sec  1.41 KBytes  11.6 Kbits/sec
[  5]   1.00-2.00   sec  0.00 Bytes  0.00 bits/sec
[  5]   2.00-3.00   sec  0.00 Bytes  0.00 bits/sec
[  5]   3.00-4.00   sec  0.00 Bytes  0.00 bits/sec
[  5]   4.00-5.00   sec  0.00 Bytes  0.00 bits/sec
[  5]   5.00-6.00   sec  0.00 Bytes  0.00 bits/sec
[  5]   6.00-7.00   sec  0.00 Bytes  0.00 bits/sec
[  5]   7.00-8.00   sec  0.00 Bytes  0.00 bits/sec
[  5]   8.00-9.00   sec  0.00 Bytes  0.00 bits/sec
[  5]   9.00-10.00  sec  0.00 Bytes  0.00 bits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-10.00  sec  1.41 KBytes  1.16 Kbits/sec
[  5]   0.00-10.09  sec  1.41 KBytes  1.15 Kbits/sec

iperf Done.
```

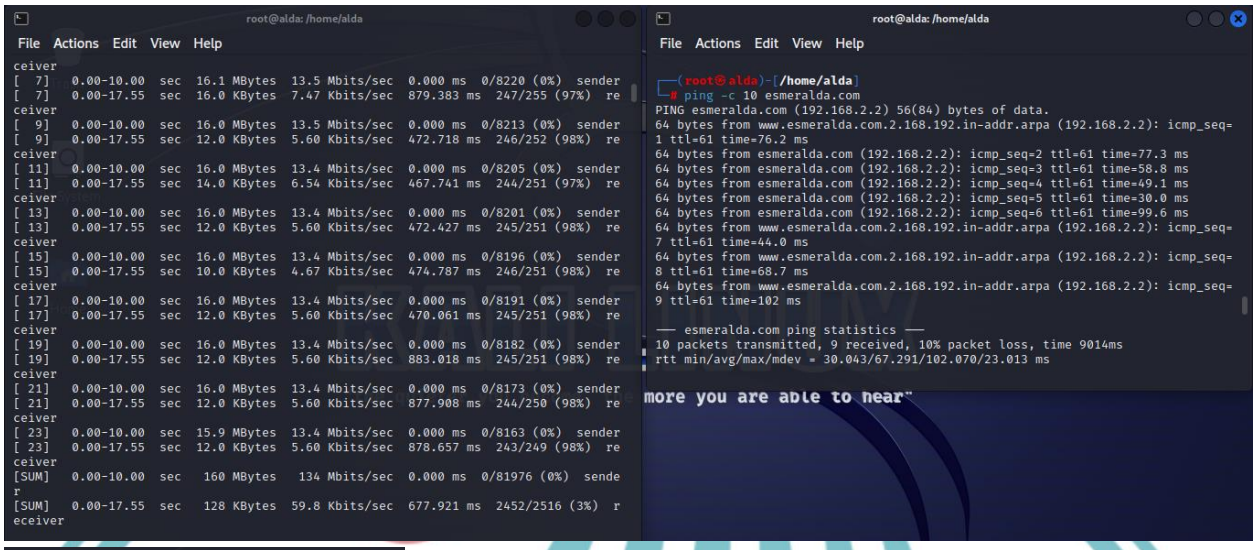
Screenshot hasil pengujian *sniffing* protokol BGP dengan *bandwidth* 50M.

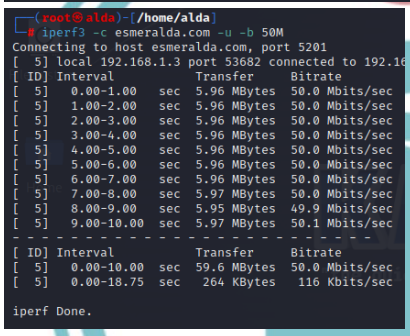
```
root@alda: /home/alda
File  Actions  Edit  View  Help

┌──(root㉿alda)-[/home/alda]
└─# iperf3 -c esmeralda.com -u -b 50M -i 60 -w 56K -l 2K -P 10
warning: UDP block size 2048 exceeds TCP MSS 1448, may result in fragmentation / dr
ops
Connecting to host esmeralda.com, port 5201
[  5] local 192.168.1.3 port 48120 connected to 192.168.2.2 port 5201
[  7] local 192.168.1.3 port 53323 connected to 192.168.2.2 port 5201
[  9] local 192.168.1.3 port 37288 connected to 192.168.2.2 port 5201
[ 11] local 192.168.1.3 port 42651 connected to 192.168.2.2 port 5201
[ 13] local 192.168.1.3 port 41669 connected to 192.168.2.2 port 5201
[ 15] local 192.168.1.3 port 58608 connected to 192.168.2.2 port 5201
[ 17] local 192.168.1.3 port 47344 connected to 192.168.2.2 port 5201
[ 19] local 192.168.1.3 port 56139 connected to 192.168.2.2 port 5201
[ 21] local 192.168.1.3 port 45723 connected to 192.168.2.2 port 5201
[ 23] local 192.168.1.3 port 42929 connected to 192.168.2.2 port 5201
[ ID] Interval           Transfer     Bitrate         Total Datagrams
[  5]   0.00-10.00  sec  16.1 MBytes  13.5 Mbits/sec  8232
[  7]   0.00-10.00  sec  16.1 MBytes  13.5 Mbits/sec  8220
[  9]   0.00-10.00  sec  16.0 MBytes  13.5 Mbits/sec  8213
[ 11]   0.00-10.00  sec  16.0 MBytes  13.4 Mbits/sec  8205
[ 13]   0.00-10.00  sec  16.0 MBytes  13.4 Mbits/sec  8201
[ 15]   0.00-10.00  sec  16.0 MBytes  13.4 Mbits/sec  8196
[ 17]   0.00-10.00  sec  16.0 MBytes  13.4 Mbits/sec  8191
[ 19]   0.00-10.00  sec  16.0 MBytes  13.4 Mbits/sec  8182
[ 21]   0.00-10.00  sec  16.0 MBytes  13.4 Mbits/sec  8173
[ 23]   0.00-10.00  sec  15.9 MBytes  13.4 Mbits/sec  8163
[SUM]   0.00-10.00  sec   160 MBytes   134 Mbits/sec  81976
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datagram
s
[  5]   0.00-10.00  sec  16.1 MBytes  13.5 Mbits/sec  0.000 ms  0/8232 (0%)  sender
[  5]   0.00-17.55  sec  16.0 KBytes  7.47 Kbits/sec  902.509 ms  247/255 (97%)  re
```

```
root@alda: /home/alda
File  Actions  Edit  View  Help

┌──(root㉿alda)-[/home/alda]
└─# ping -c 10 esmeralda.com
PING esmeralda.com (192.168.2.2) 56(84) bytes of data.
64 bytes from www.esmeralda.com.2.168.192.in-addr.arpa (192.168.2.2): icmp_seq=
1 ttl=61 time=76.2 ms
64 bytes from esmeralda.com (192.168.2.2): icmp_seq=2 ttl=61 time=77.3 ms
64 bytes from esmeralda.com (192.168.2.2): icmp_seq=3 ttl=61 time=58.8 ms
64 bytes from esmeralda.com (192.168.2.2): icmp_seq=4 ttl=61 time=49.1 ms
64 bytes from esmeralda.com (192.168.2.2): icmp_seq=5 ttl=61 time=30.0 ms
64 bytes from esmeralda.com (192.168.2.2): icmp_seq=6 ttl=61 time=99.6 ms
64 bytes from www.esmeralda.com.2.168.192.in-addr.arpa (192.168.2.2): icmp_seq=
7 ttl=61 time=44.0 ms
64 bytes from www.esmeralda.com.2.168.192.in-addr.arpa (192.168.2.2): icmp_seq=
8 ttl=61 time=68.7 ms
64 bytes from www.esmeralda.com.2.168.192.in-addr.arpa (192.168.2.2): icmp_seq=
9 ttl=61 time=102 ms

── esmeralda.com ping statistics ──
10 packets transmitted, 9 received, 10% packet loss, time 9014ms
rtt min/avg/max/mdev = 30.043/67.291/102.070/23.013 ms

more you are able to hear"
```

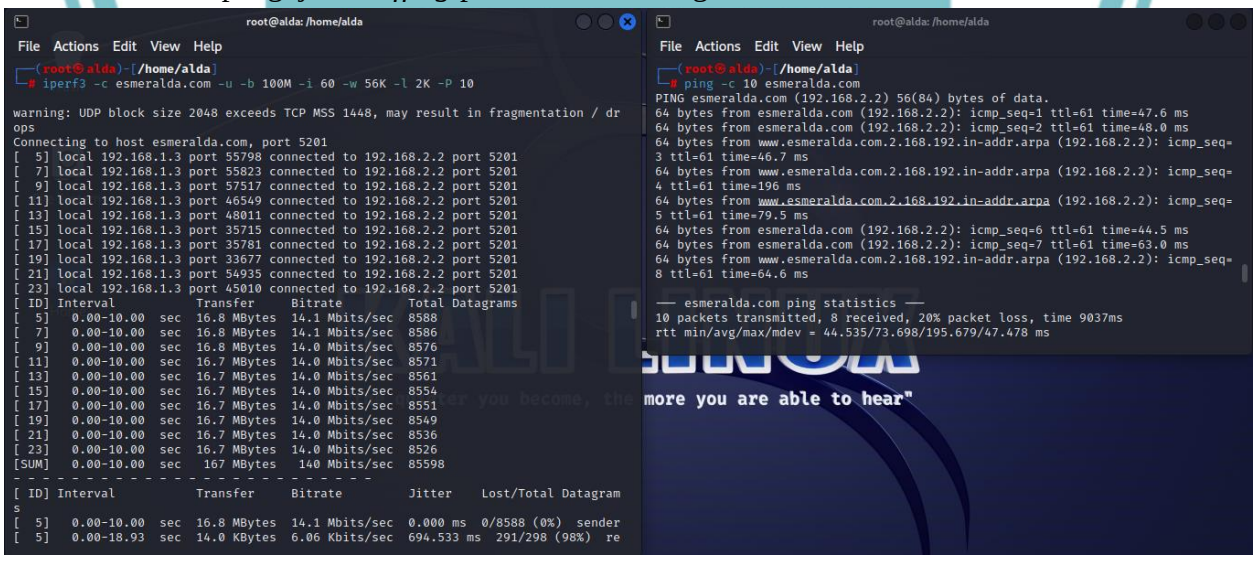
```
root@alda: /home/alda
File  Actions  Edit  View  Help

[ 13]   0.00-10.00  sec  16.0 MBytes  13.4 Mbits/sec  8201
[ 15]   0.00-10.00  sec  16.0 MBytes  13.4 Mbits/sec  8196
[ 17]   0.00-10.00  sec  16.0 MBytes  13.4 Mbits/sec  8191
[ 19]   0.00-10.00  sec  16.0 MBytes  13.4 Mbits/sec  8182
[ 21]   0.00-10.00  sec  16.0 MBytes  13.4 Mbits/sec  8173
[ 23]   0.00-10.00  sec  15.9 MBytes  13.4 Mbits/sec  8163
[SUM]   0.00-10.00  sec   160 MBytes   134 Mbits/sec  81976
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datagram
s
[  5]   0.00-10.00  sec  16.1 MBytes  13.5 Mbits/sec  0.000 ms  0/8232 (0%)  sender
[  5]   0.00-17.55  sec  16.0 KBytes  7.47 Kbits/sec  902.509 ms  247/255 (97%)  re
ceiver
[  7]   0.00-10.00  sec  16.1 MBytes  13.5 Mbits/sec  0.000 ms  0/8220 (0%)  sender
[  7]   0.00-17.55  sec  16.0 KBytes  7.47 Kbits/sec  879.383 ms  247/255 (97%)  re
ceiver
[  9]   0.00-10.00  sec  16.0 MBytes  13.5 Mbits/sec  0.000 ms  0/8213 (0%)  sender
[  9]   0.00-17.55  sec  12.0 KBytes  5.60 Kbits/sec  472.718 ms  246/252 (98%)  re
ceiver
[ 11]   0.00-10.00  sec  16.0 MBytes  13.4 Mbits/sec  0.000 ms  0/8205 (0%)  sender
[ 11]   0.00-17.55  sec  14.0 KBytes  6.54 Kbits/sec  467.741 ms  244/251 (97%)  re
ceiver
[ 13]   0.00-10.00  sec  16.0 MBytes  13.4 Mbits/sec  0.000 ms  0/8201 (0%)  sender
[ 13]   0.00-17.55  sec  12.0 KBytes  5.60 Kbits/sec  472.427 ms  245/251 (98%)  re
ceiver
[ 15]   0.00-10.00  sec  16.0 MBytes  13.4 Mbits/sec  0.000 ms  0/8196 (0%)  sender
[ 15]   0.00-17.55  sec  10.0 KBytes  4.67 Kbits/sec  474.787 ms  246/251 (98%)  re
ceiver
[ 17]   0.00-10.00  sec  16.0 MBytes  13.4 Mbits/sec  0.000 ms  0/8191 (0%)  sender
[ 17]   0.00-17.55  sec  12.0 KBytes  5.60 Kbits/sec  470.061 ms  245/251 (98%)  re
ceiver
[ 19]   0.00-10.00  sec  16.0 MBytes  13.4 Mbits/sec  0.000 ms  0/8182 (0%)  sender
[ 19]   0.00-17.55  sec  12.0 KBytes  5.60 Kbits/sec  883.018 ms  245/251 (98%)  re
```

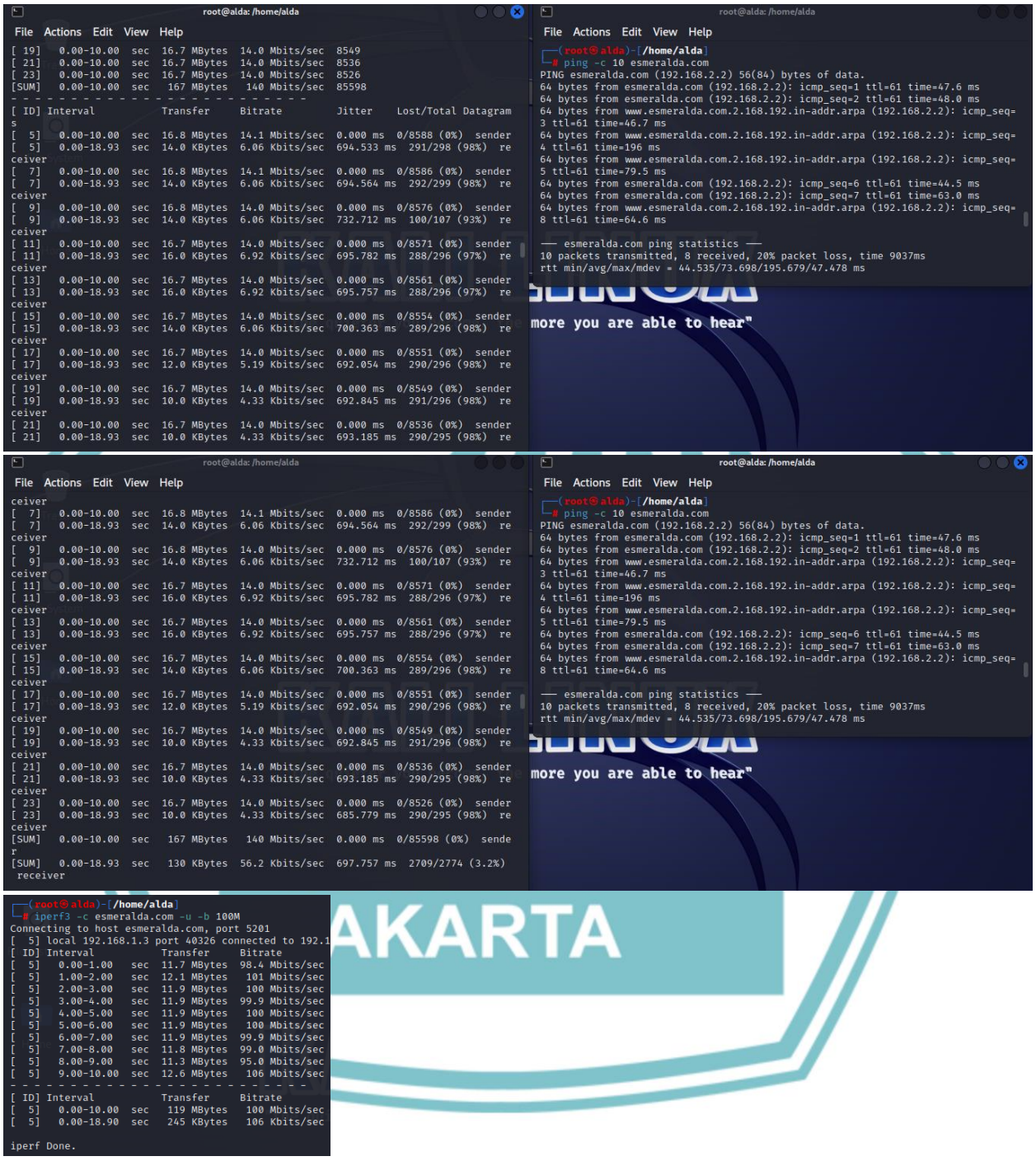
```
root@alda: /home/alda
File  Actions  Edit  View  Help

┌──(root㉿alda)-[/home/alda]
└─# ping -c 10 esmeralda.com
PING esmeralda.com (192.168.2.2) 56(84) bytes of data.
64 bytes from www.esmeralda.com.2.168.192.in-addr.arpa (192.168.2.2): icmp_seq=
1 ttl=61 time=76.2 ms
64 bytes from esmeralda.com (192.168.2.2): icmp_seq=2 ttl=61 time=77.3 ms
64 bytes from esmeralda.com (192.168.2.2): icmp_seq=3 ttl=61 time=58.8 ms
64 bytes from esmeralda.com (192.168.2.2): icmp_seq=4 ttl=61 time=49.1 ms
64 bytes from esmeralda.com (192.168.2.2): icmp_seq=5 ttl=61 time=30.0 ms
64 bytes from esmeralda.com (192.168.2.2): icmp_seq=6 ttl=61 time=99.6 ms
64 bytes from www.esmeralda.com.2.168.192.in-addr.arpa (192.168.2.2): icmp_seq=
7 ttl=61 time=44.0 ms
64 bytes from www.esmeralda.com.2.168.192.in-addr.arpa (192.168.2.2): icmp_seq=
8 ttl=61 time=68.7 ms
64 bytes from www.esmeralda.com.2.168.192.in-addr.arpa (192.168.2.2): icmp_seq=
9 ttl=61 time=102 ms

── esmeralda.com ping statistics ──
10 packets transmitted, 9 received, 10% packet loss, time 9014ms
rtt min/avg/max/mdev = 30.043/67.291/102.070/23.013 ms

more you are able to hear"
```



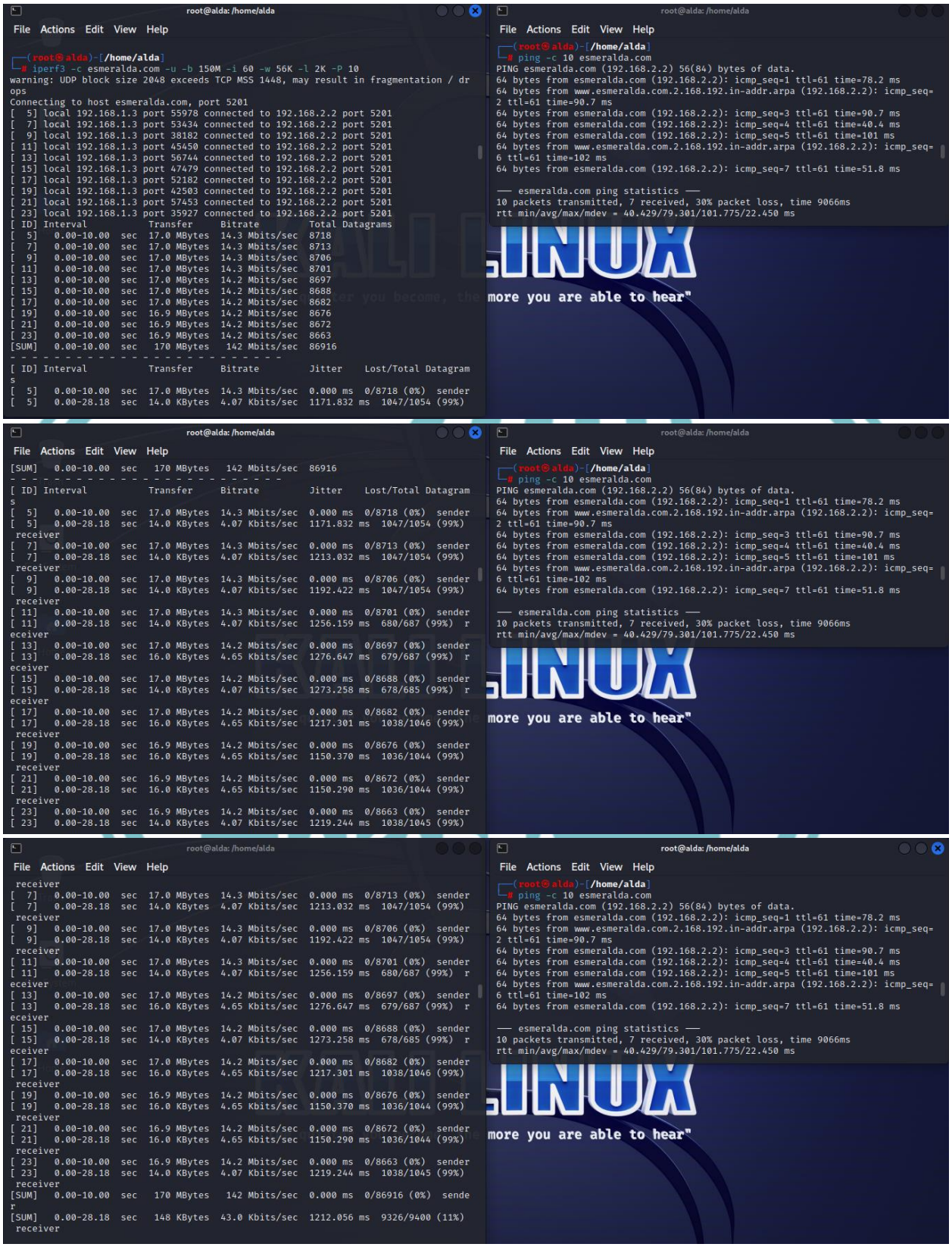


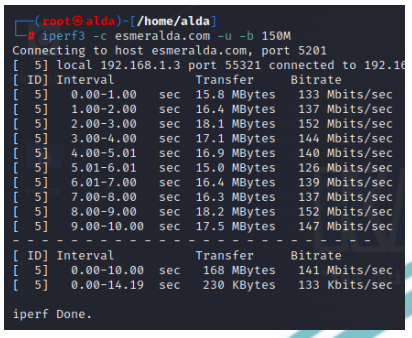
Screenshot hasil pengujian *sniffing* protokol BGP dengan *bandwidth* 100M.



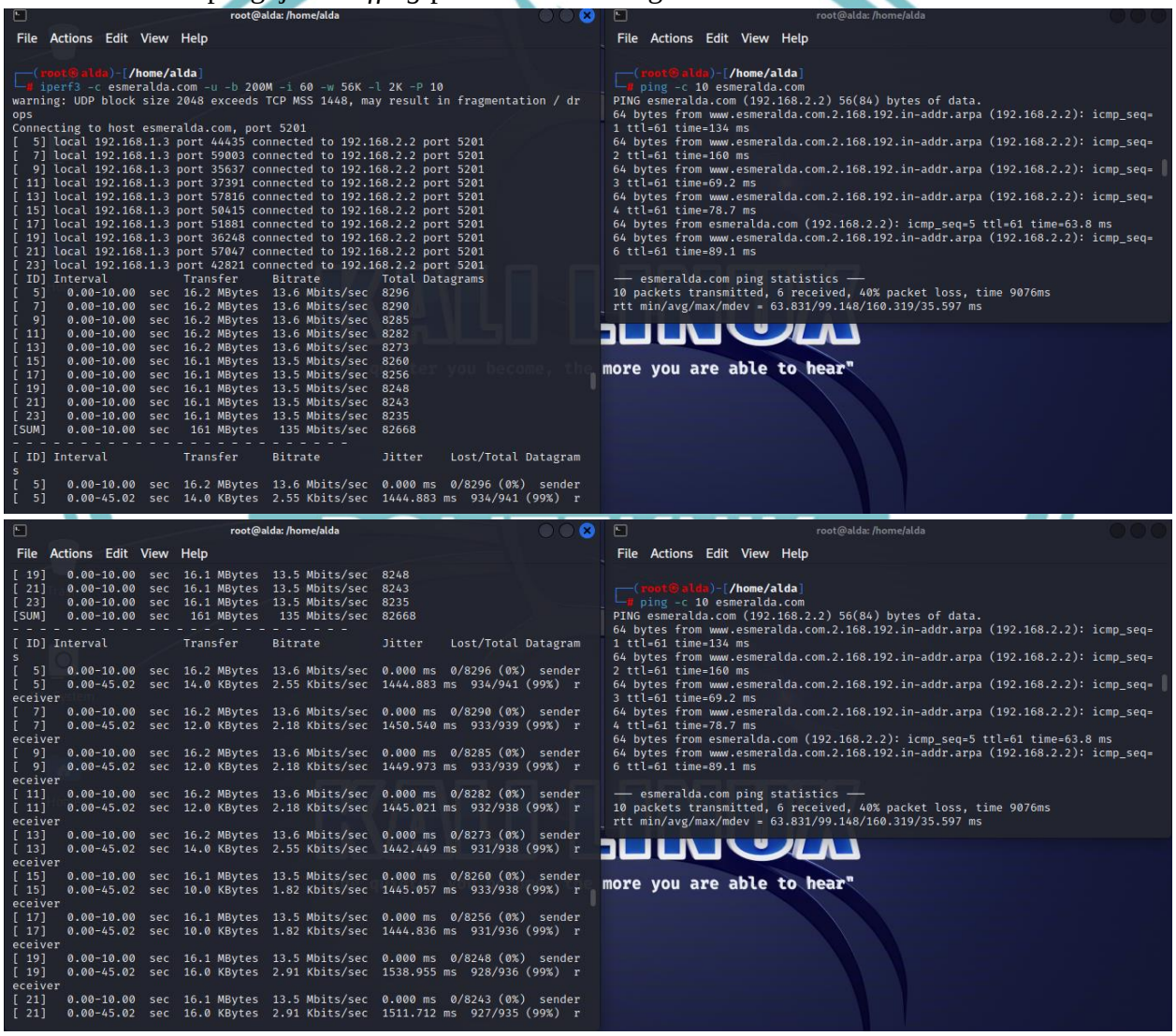


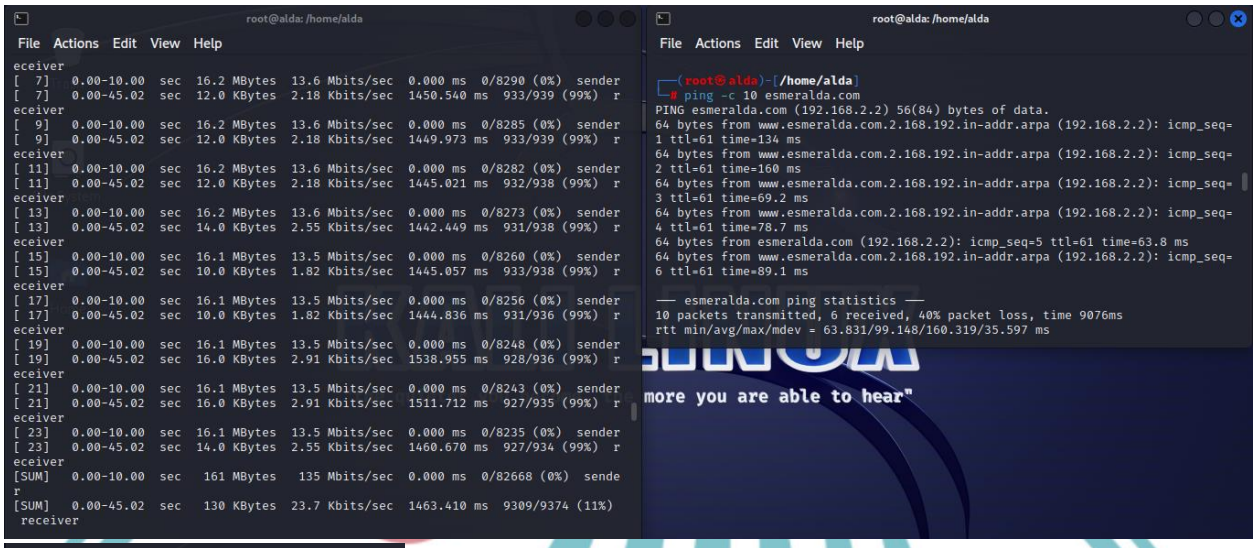
Screenshot hasil pengujian *sniffing* protokol BGP dengan *bandwidth* 150M.

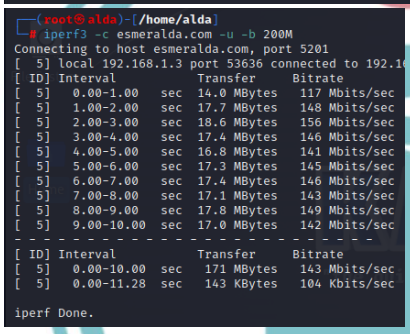




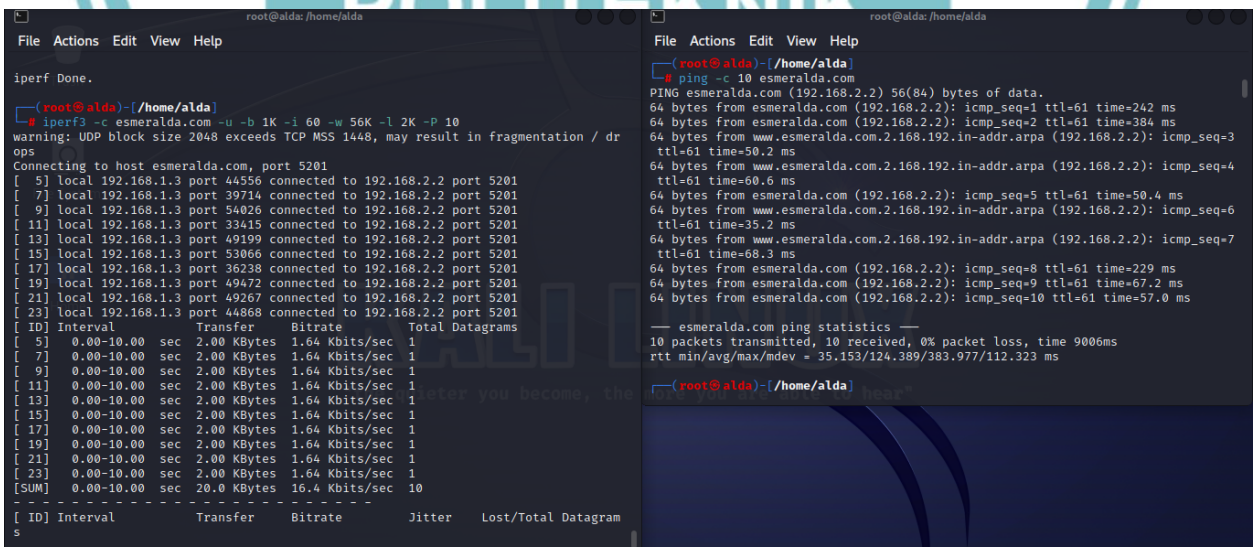
Screenshot hasil pengujian *sniffing* protokol BGP dengan *bandwidth* 200M.

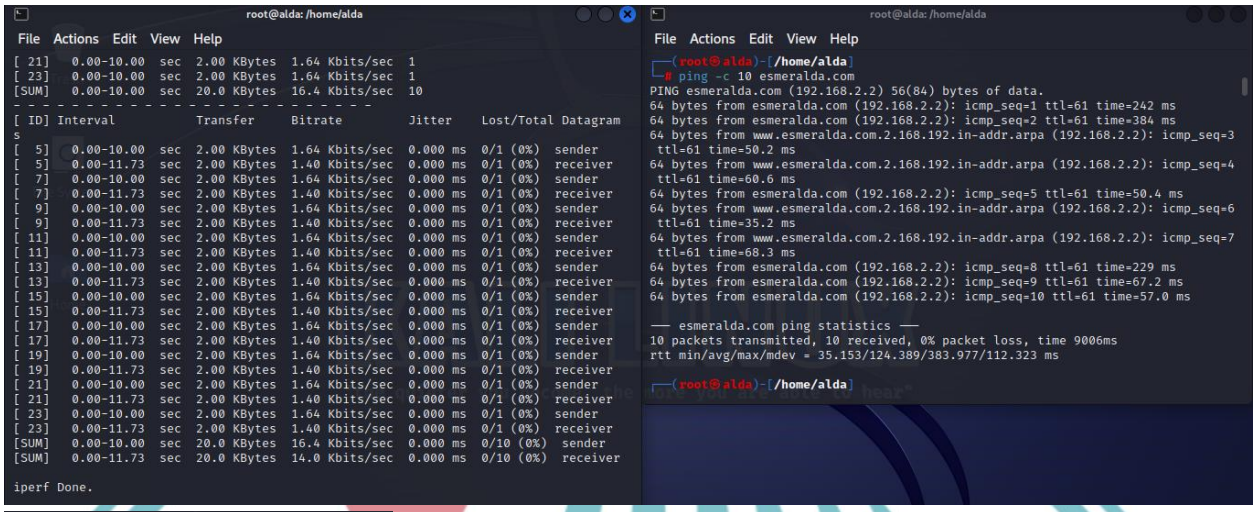


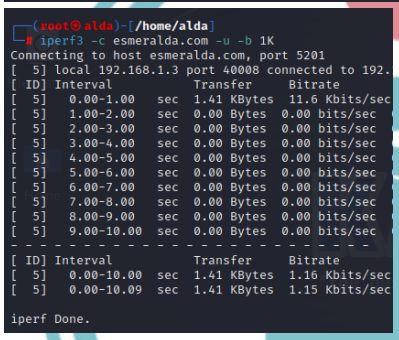




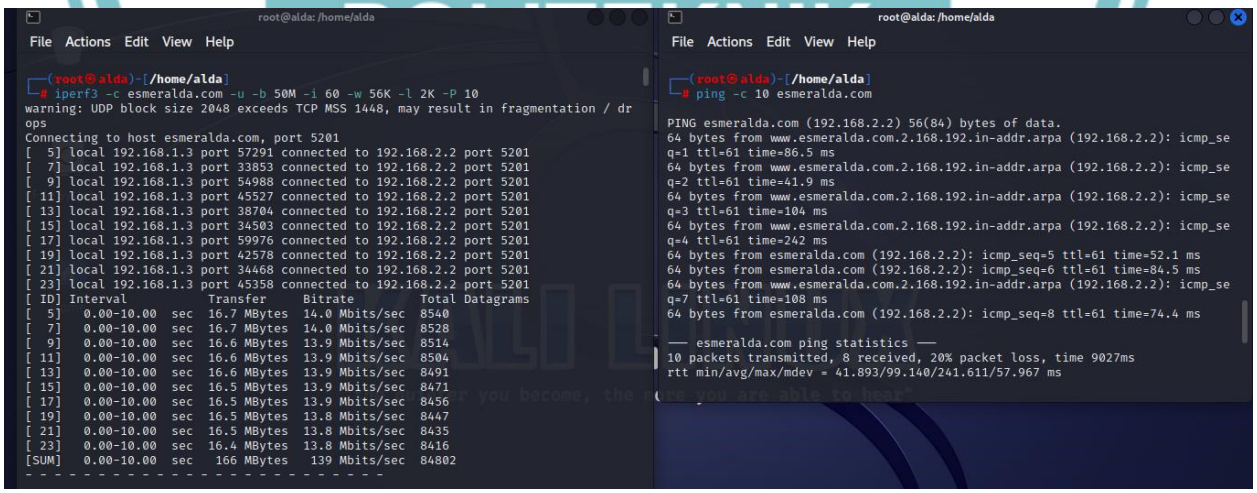
Screenshot hasil pengujian *spoofing* dan *sniffing* protokol BGP dengan *bandwidth* 1K.



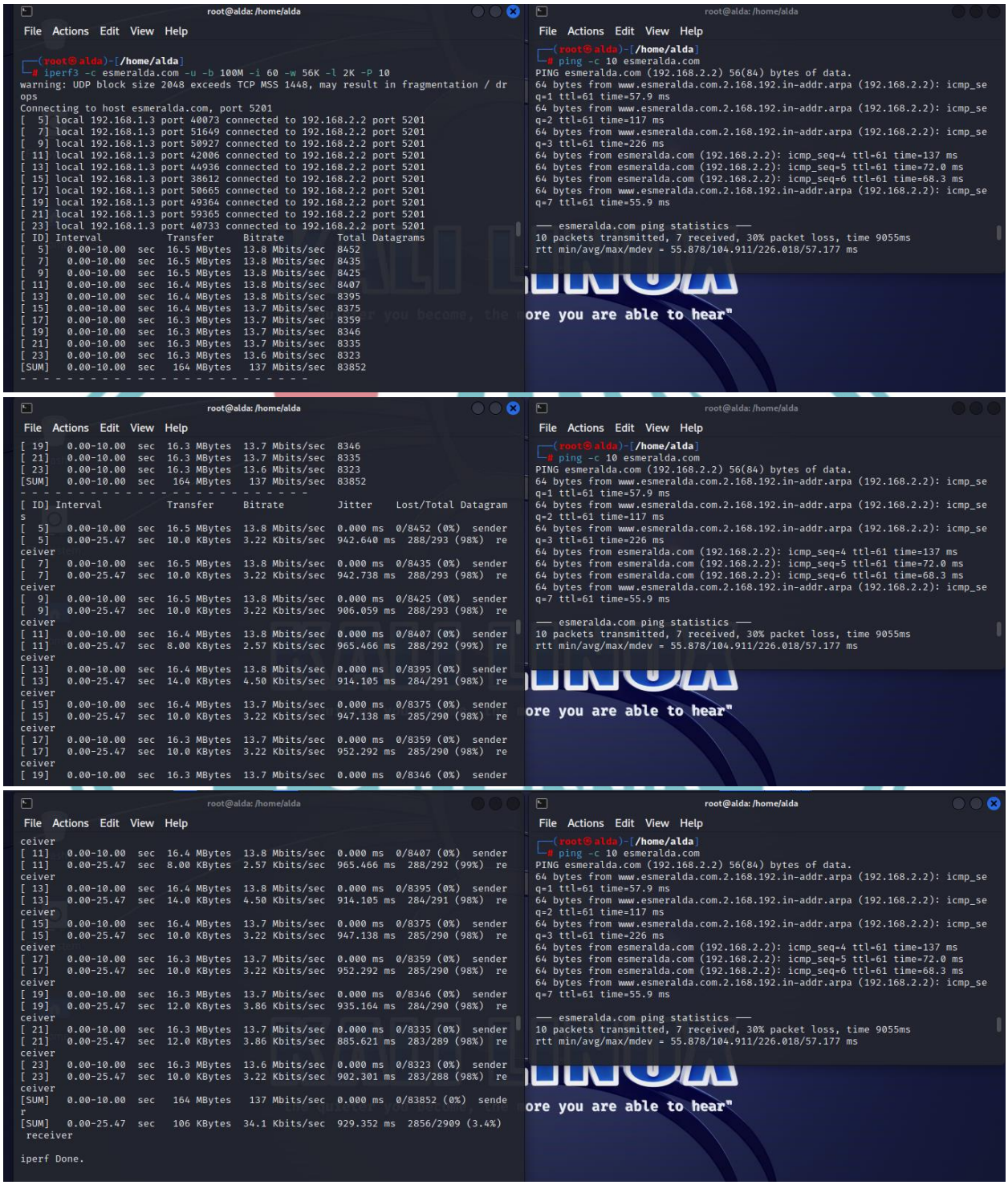


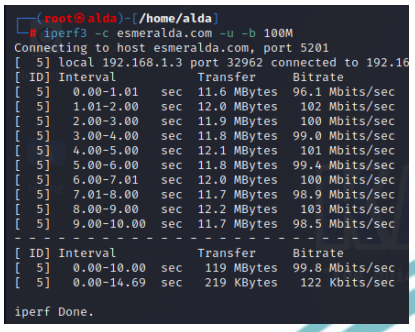


Screenshot hasil pengujian *spoofing* dan *sniffing* protokol BGP dengan *bandwidth* 50M.

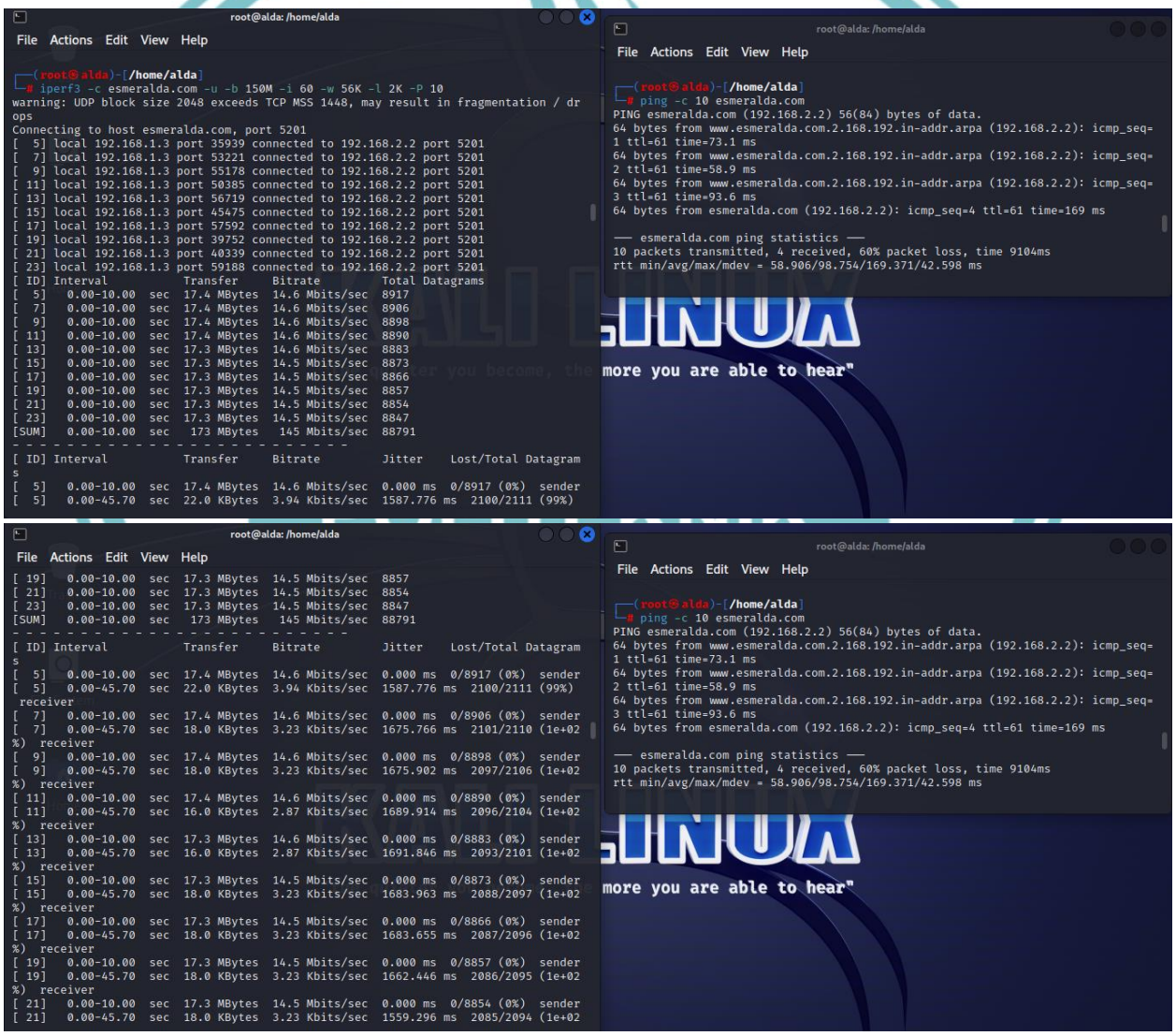


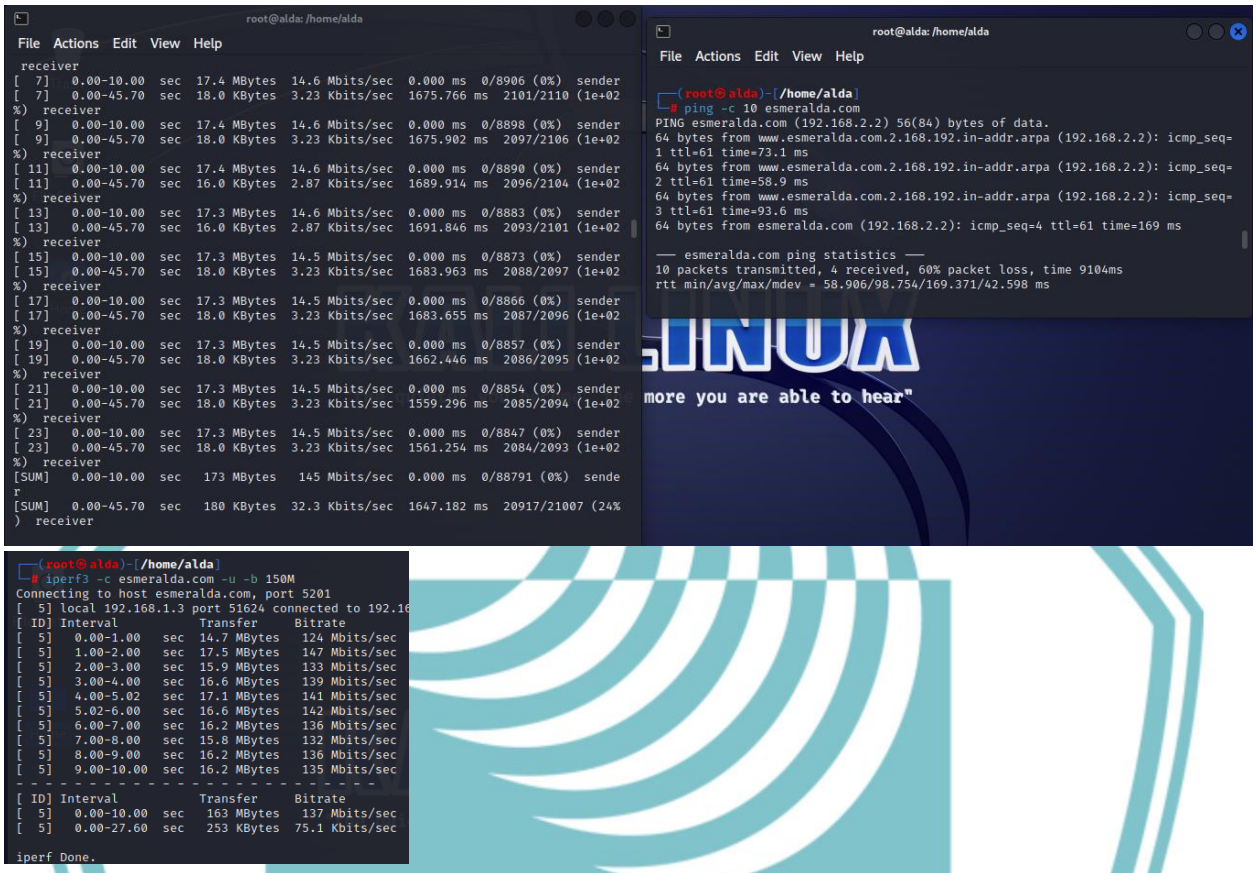
Screenshot hasil pengujian *spoofing* dan *sniffing* protokol BGP dengan *bandwidth* 100M.



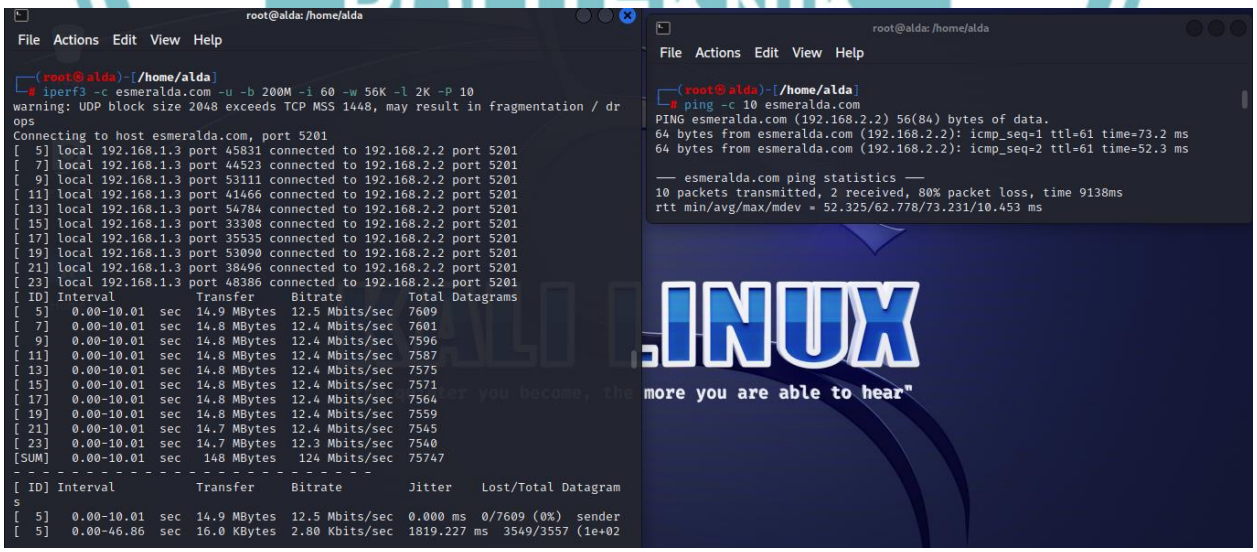


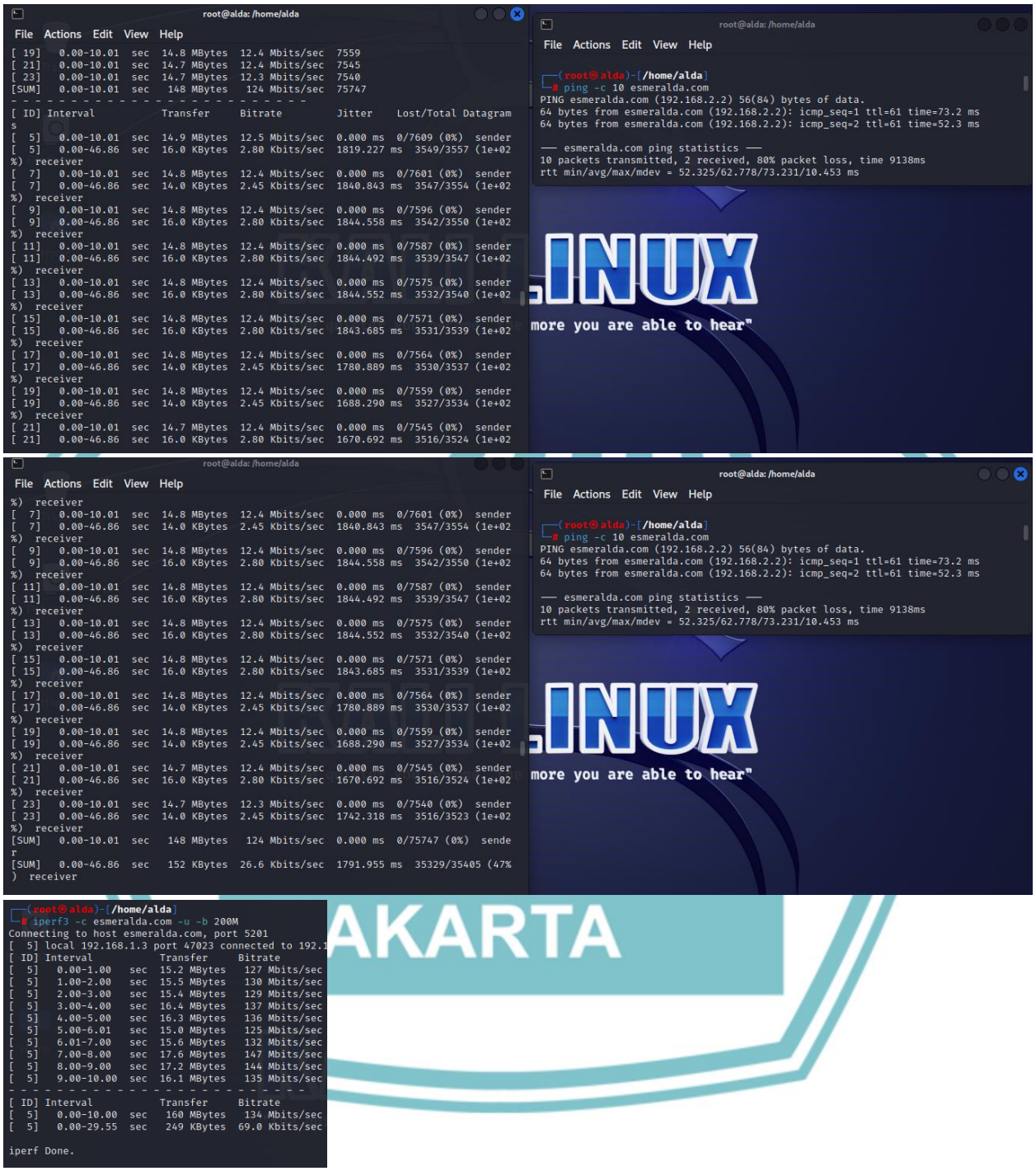
Screenshot hasil pengujian *spoofing* dan *sniffing* protokol BGP dengan *bandwidth* 150M.



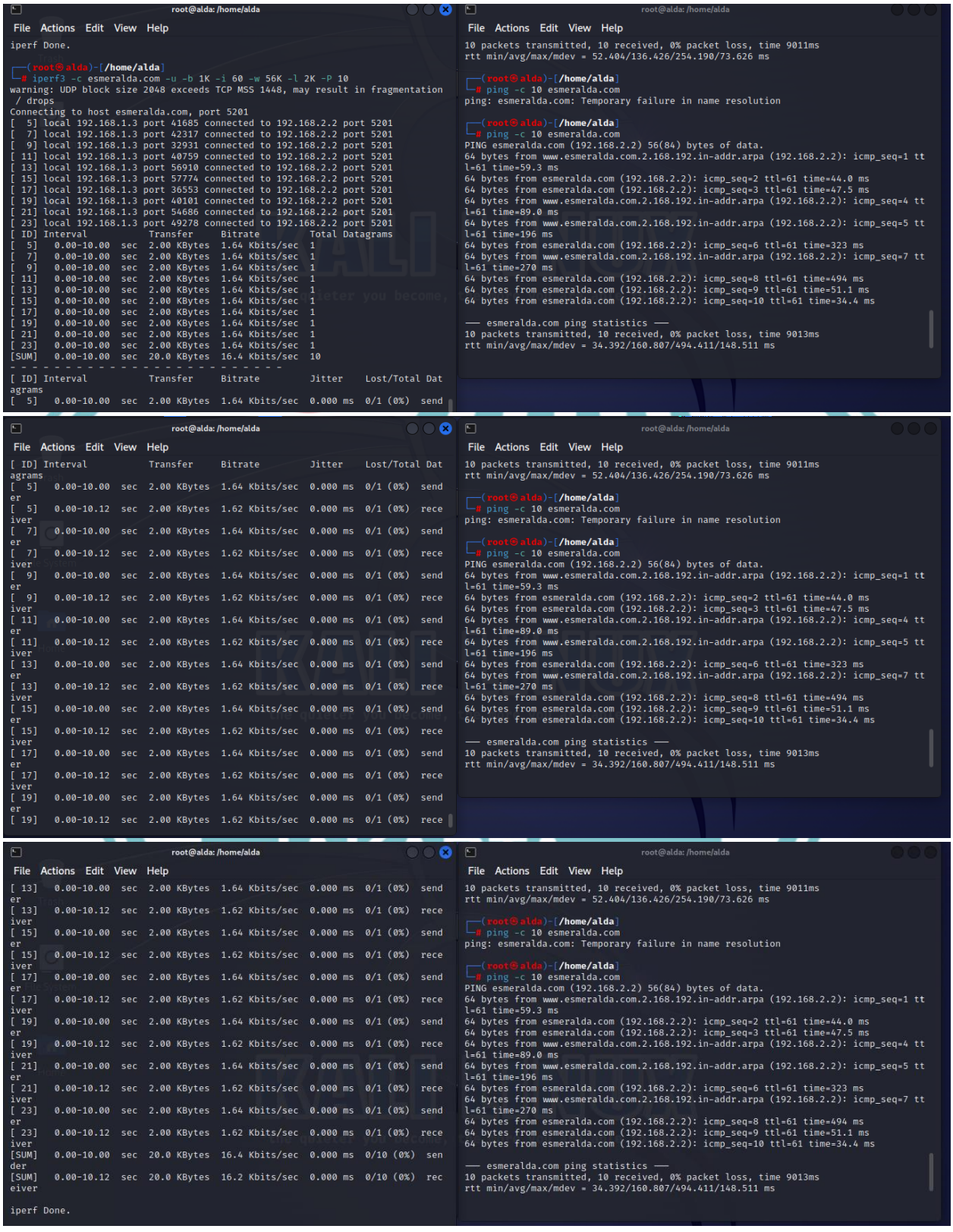


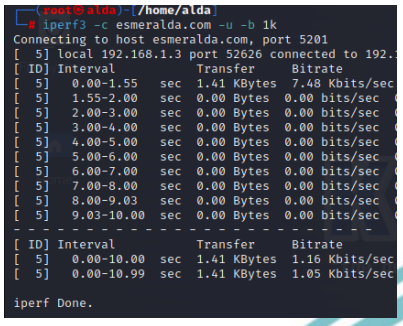
Screenshot hasil pengujian *spoofing* dan *sniffing* protokol BGP dengan *bandwidth* 200M.



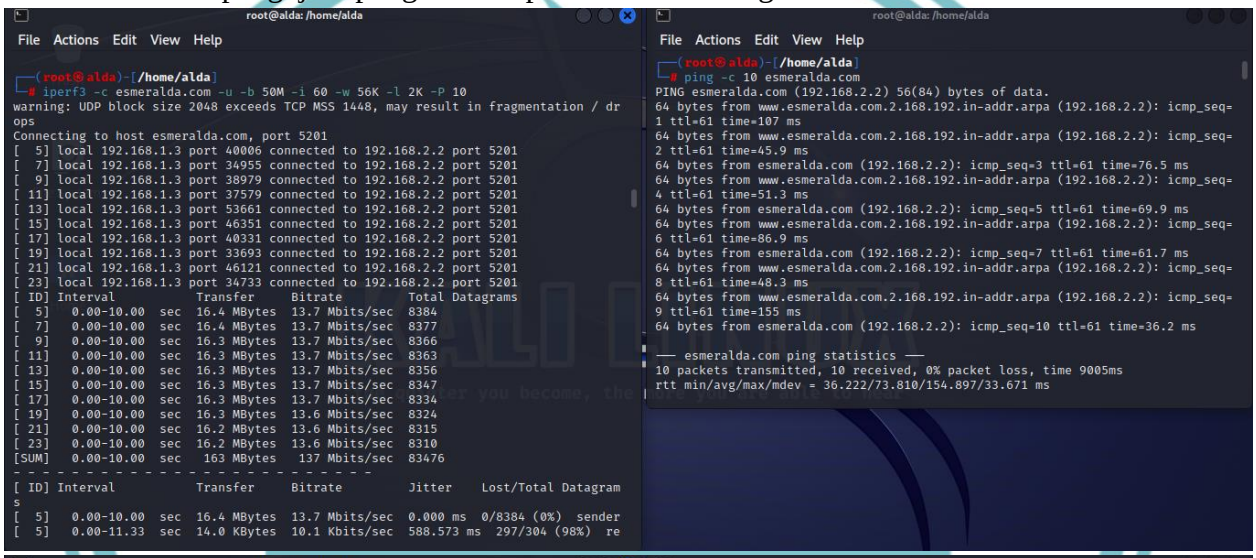


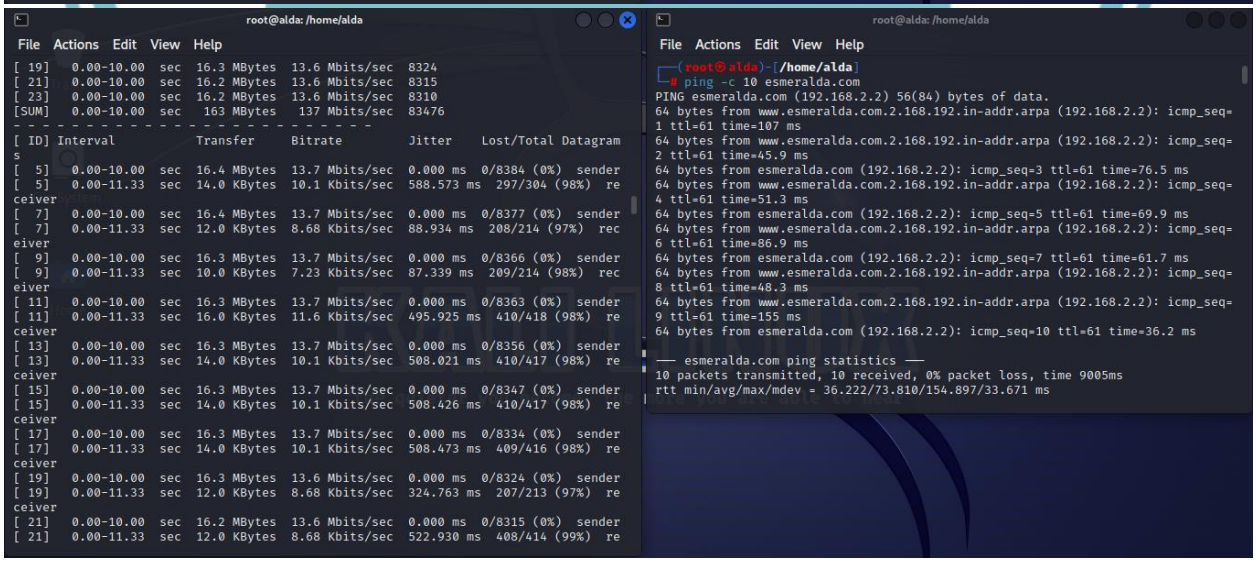
Screenshot hasil pengujian pengamanan protokol BGP dengan *bandwidth* 1K.

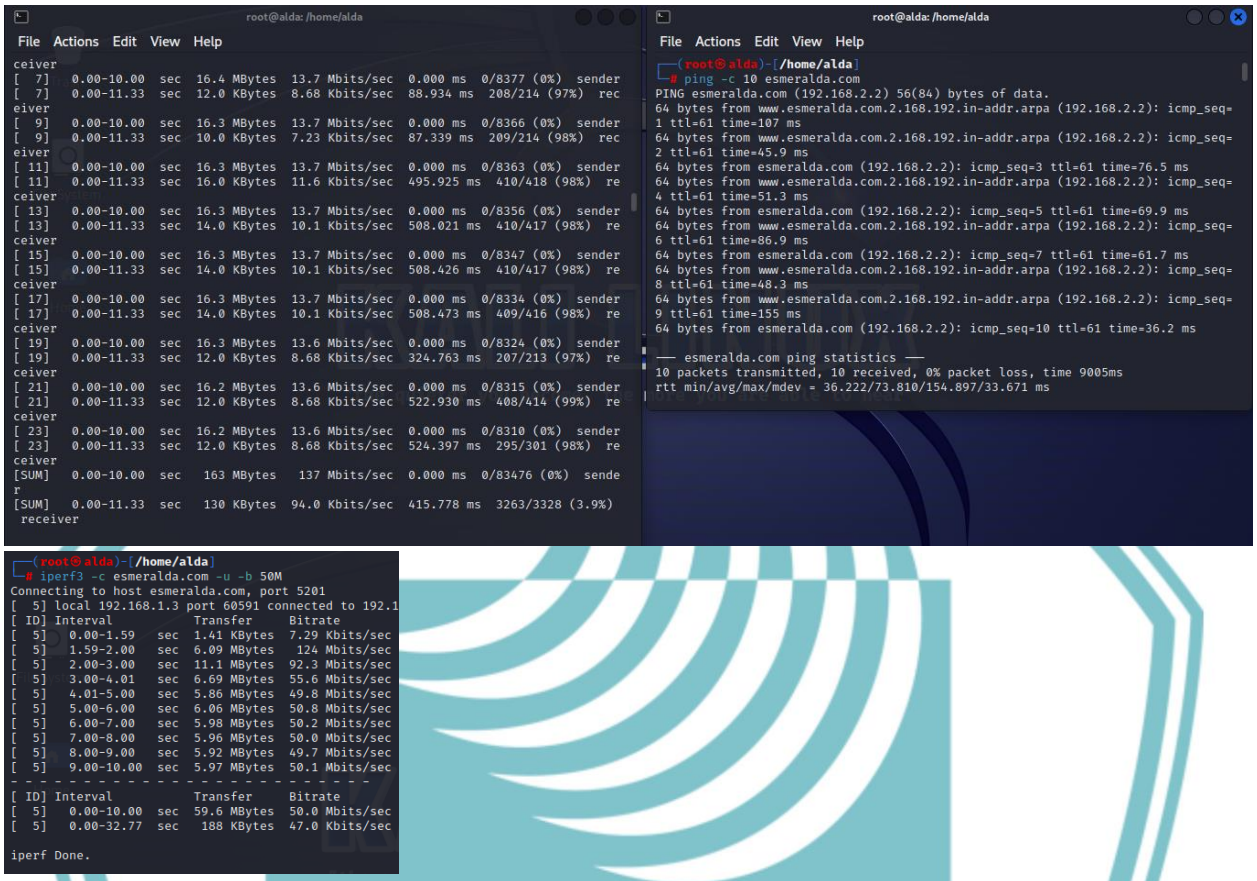




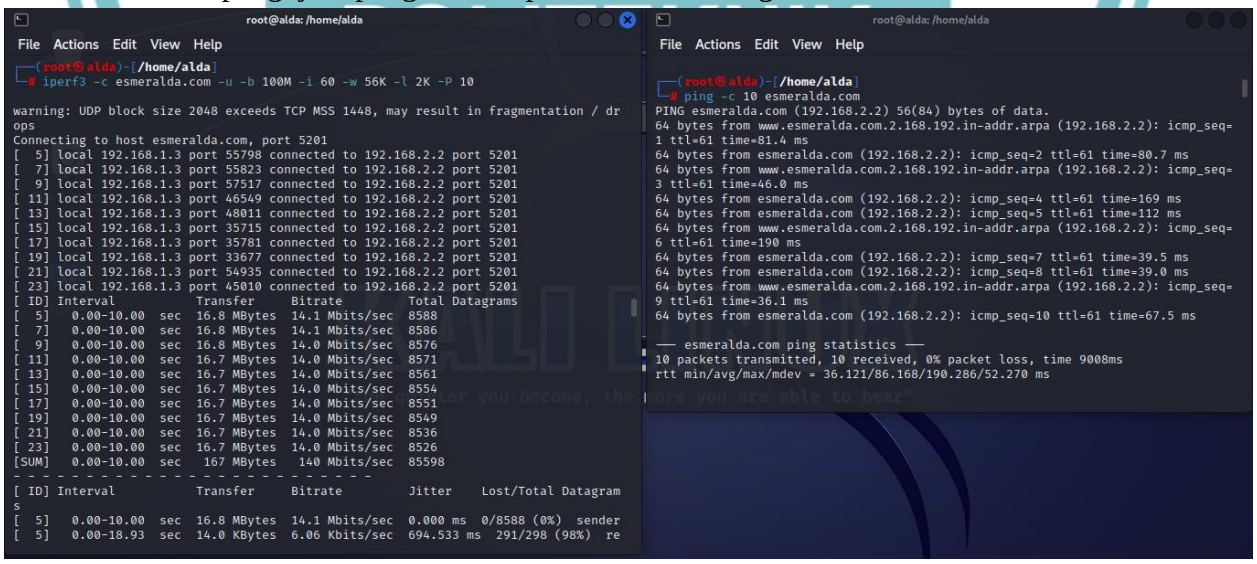
Screenshot hasil pengujian pengamanan protokol BGP dengan *bandwidth* 50M.

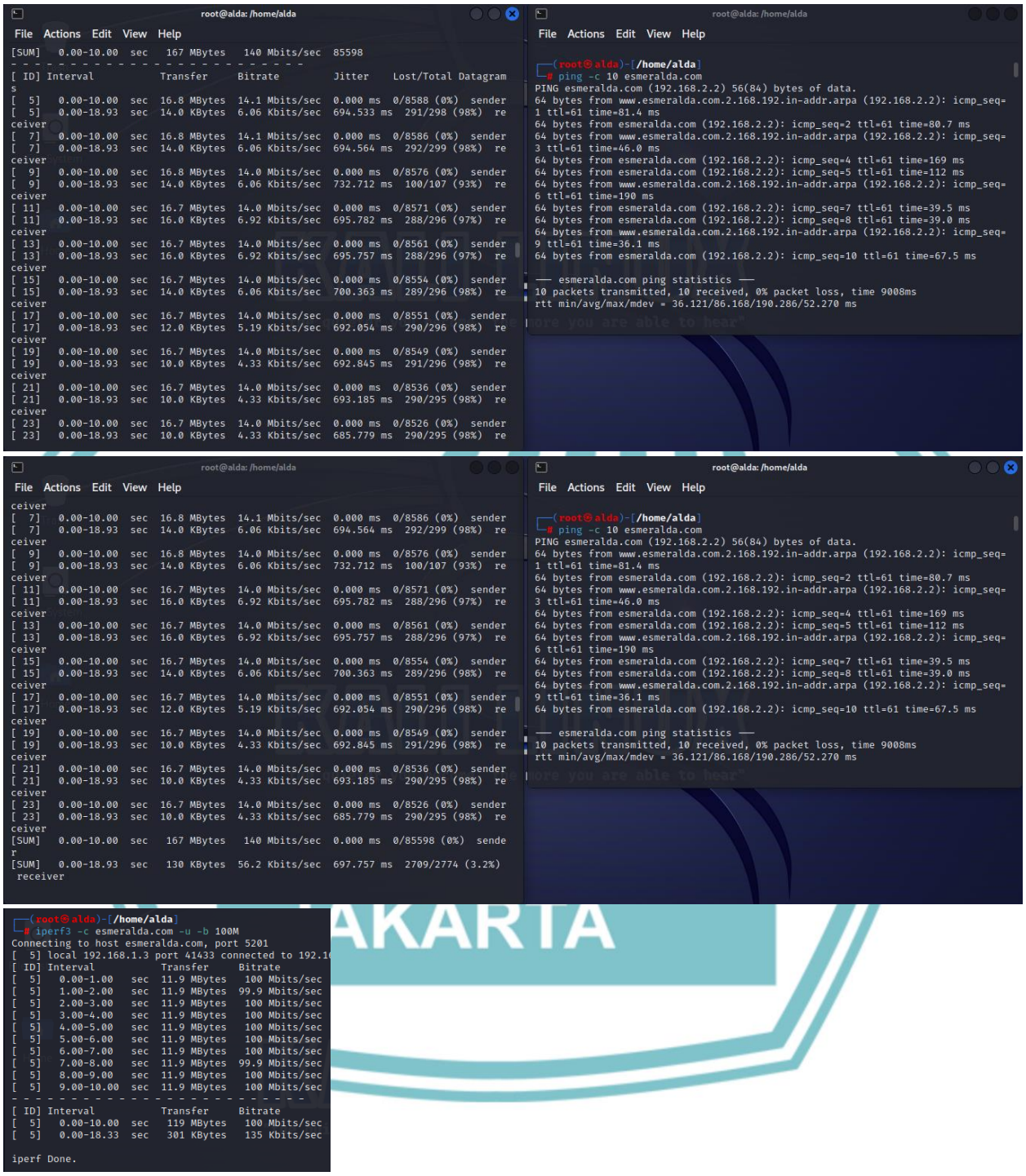




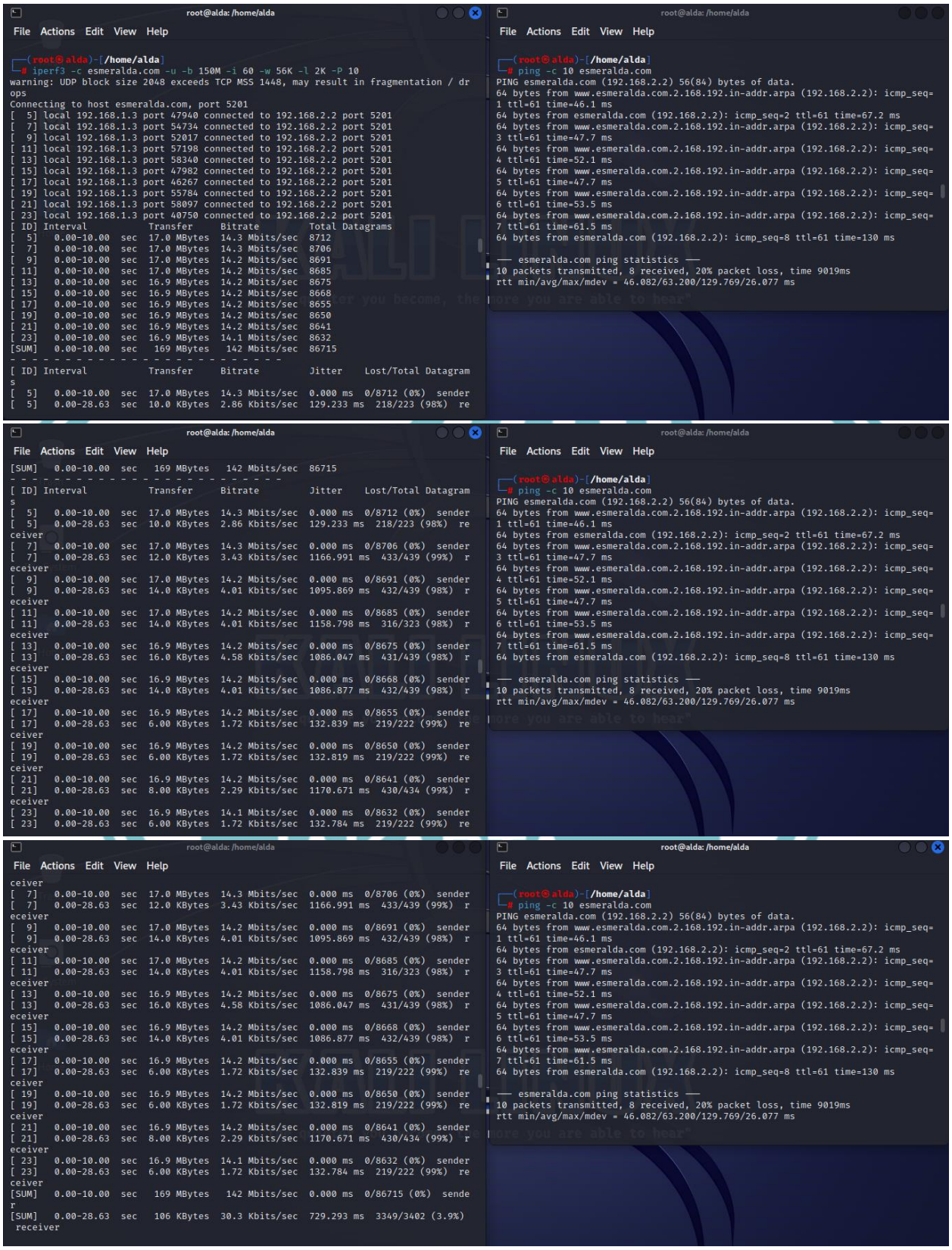


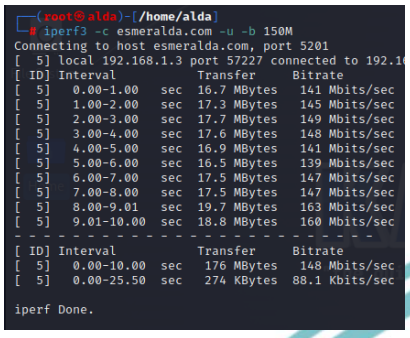
Screenshot hasil pengujian pengamanan protokol BGP dengan *bandwidth* 100M.



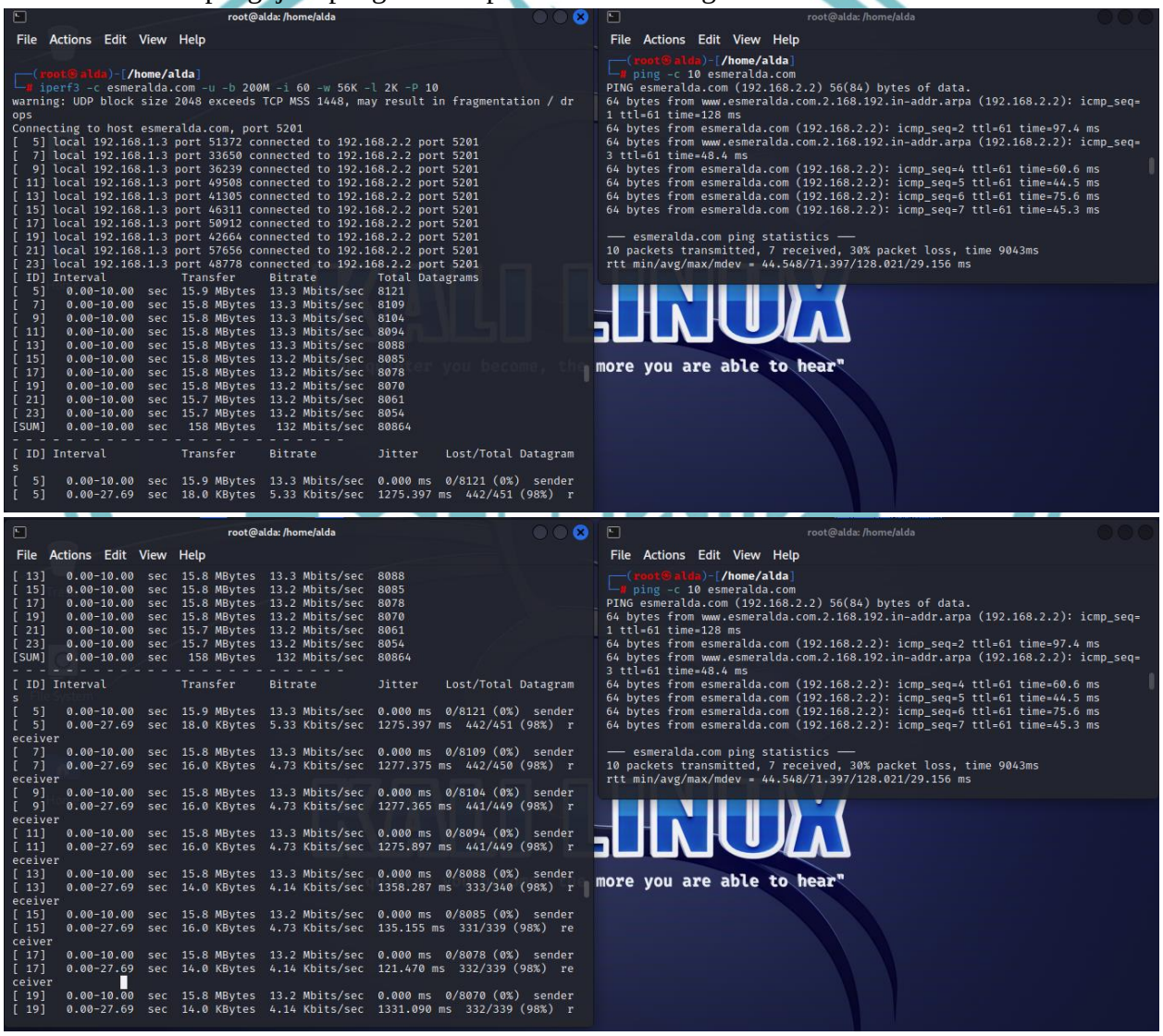


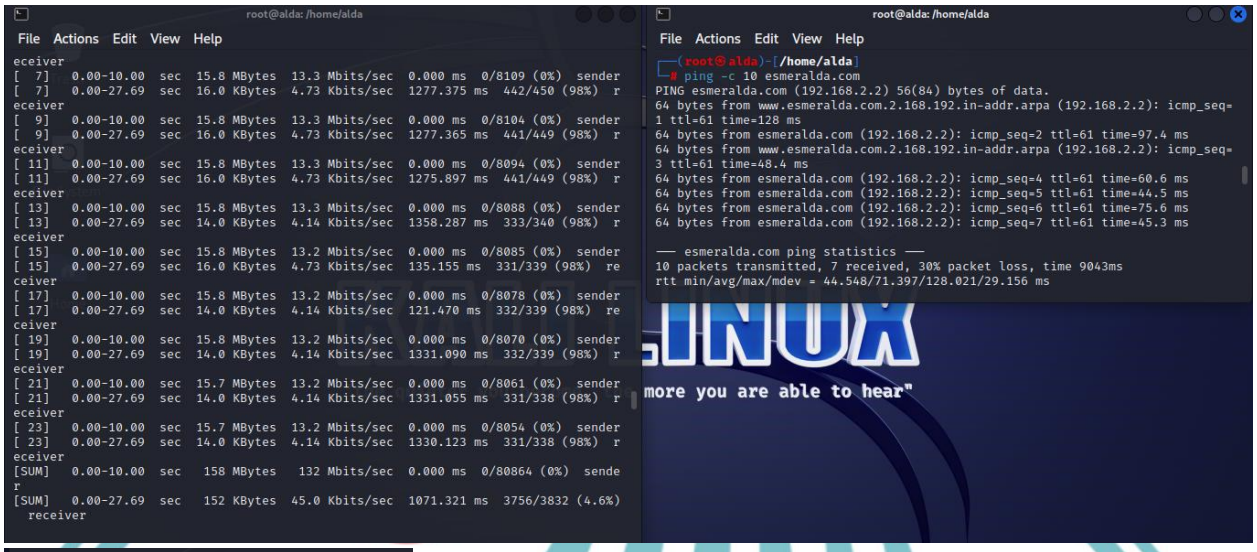
Screenshot hasil pengujian pengamanan protokol BGP dengan *bandwidth* 150M.

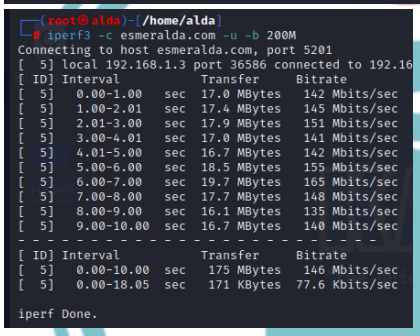




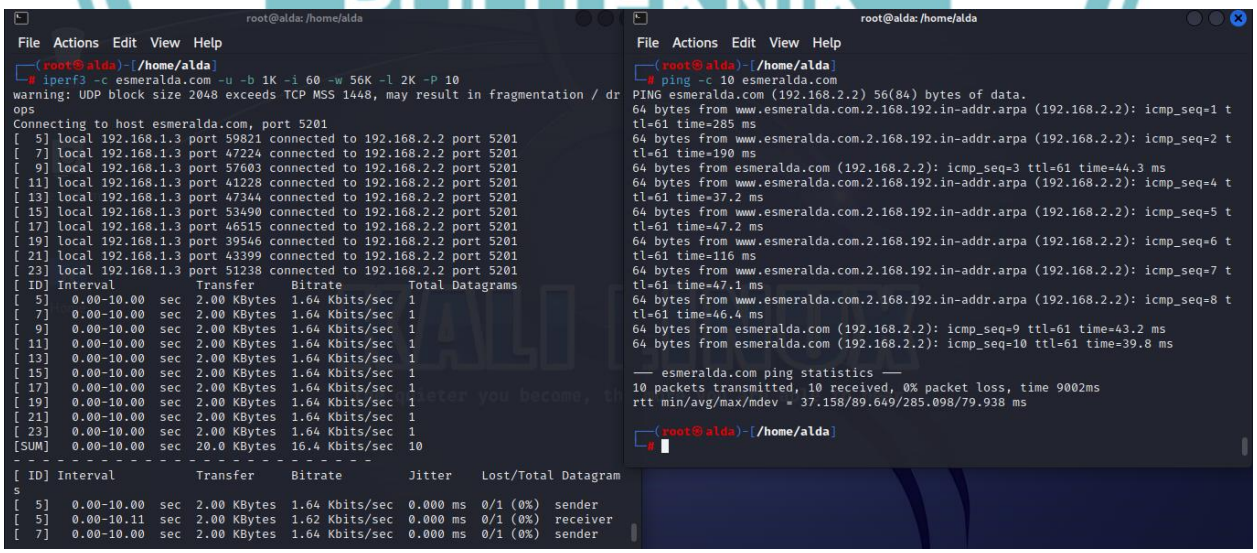
Screenshot hasil pengujian pengamanan protokol BGP dengan *bandwidth* 200M.

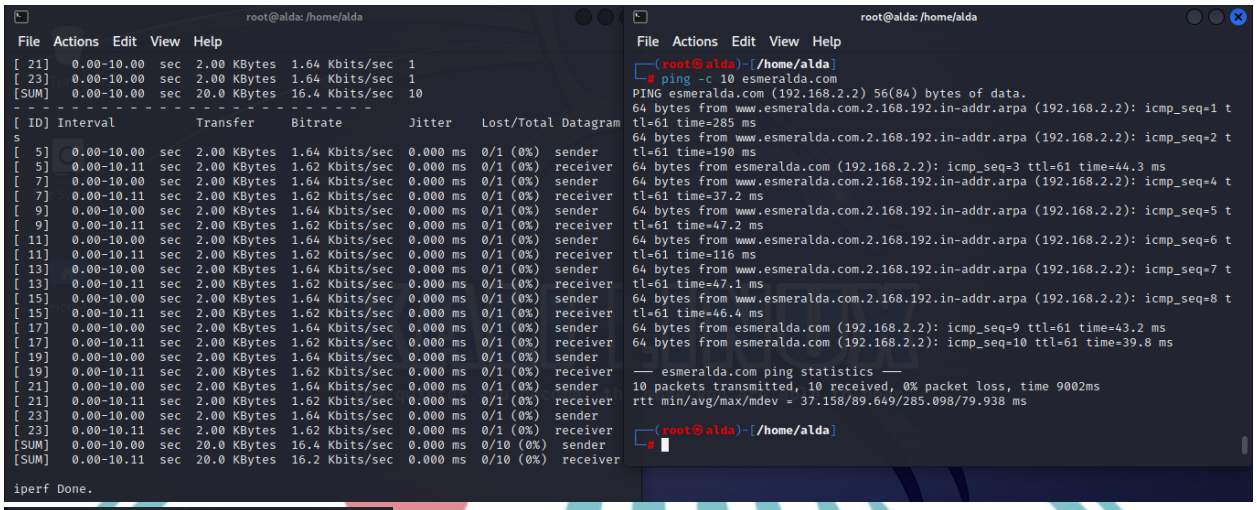


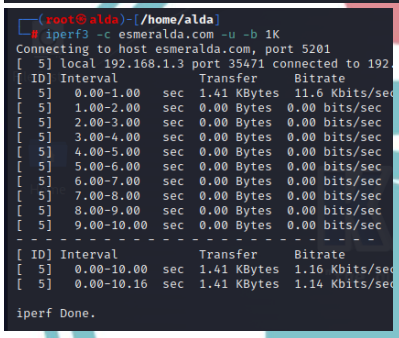




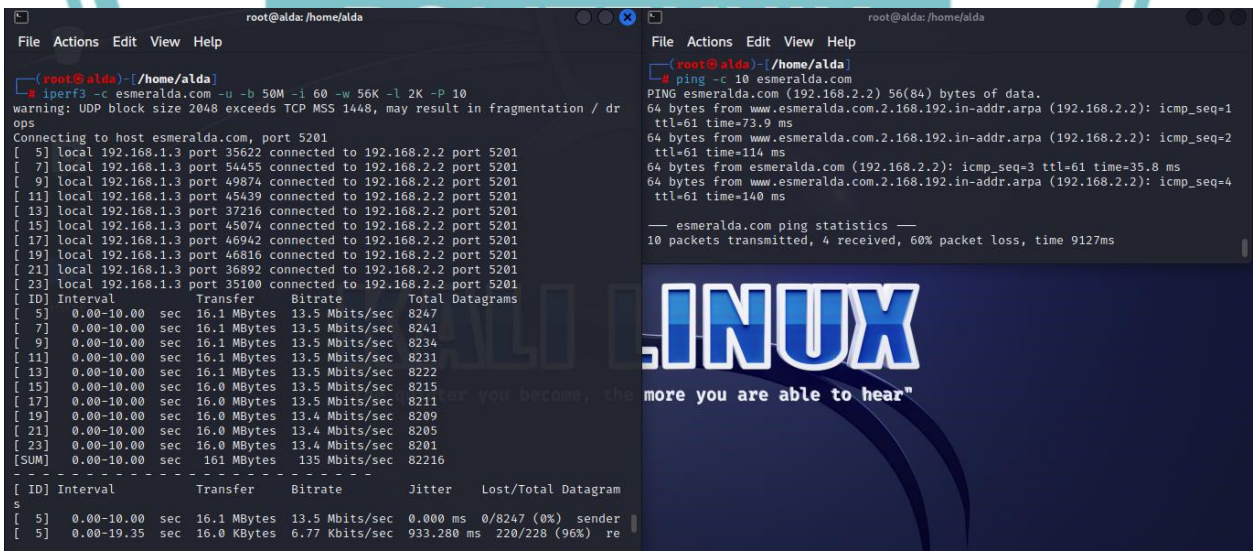
Screenshot hasil pengujian serangan *spoofing* protokol EIGRP dengan *bandwidth* 1K.



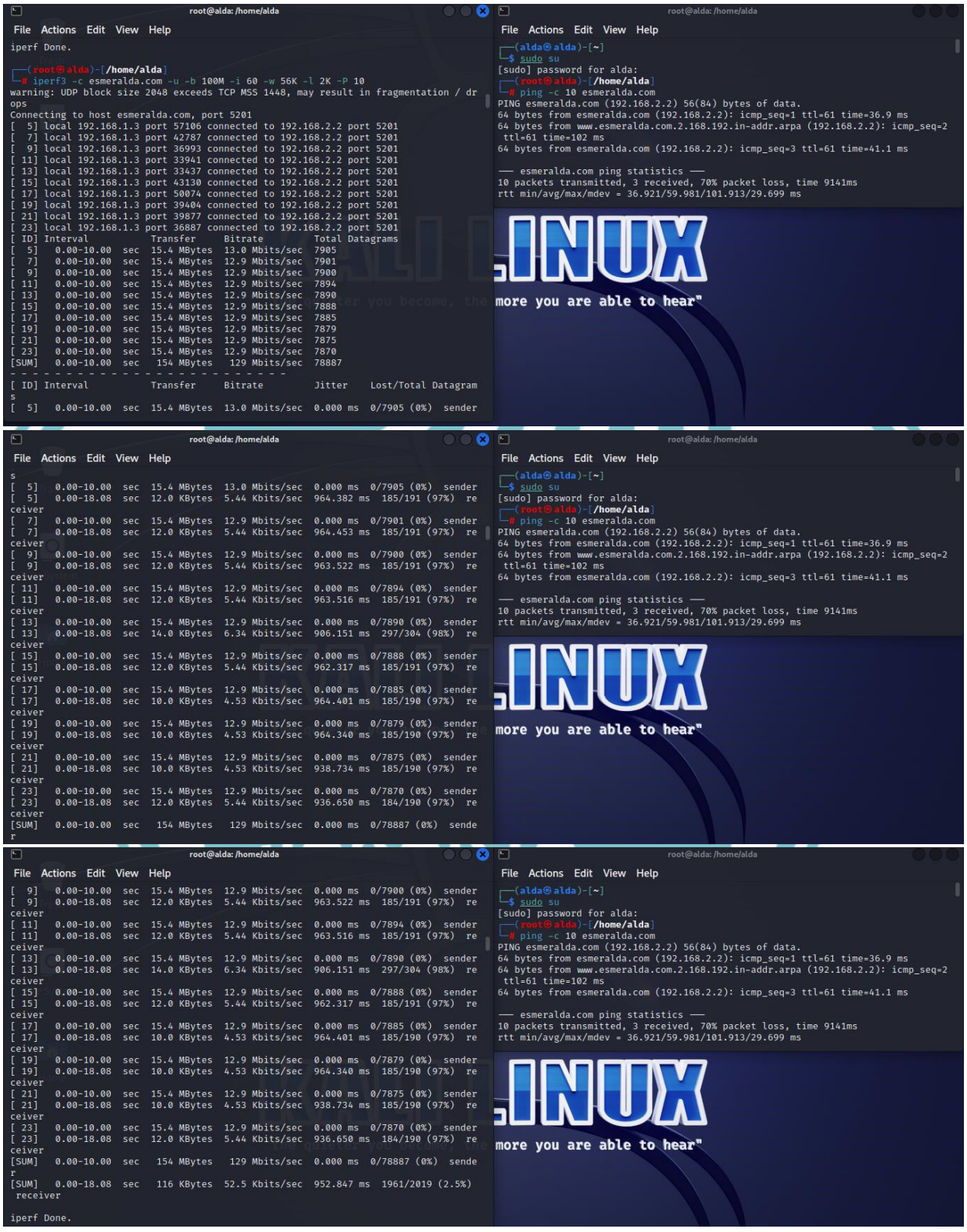




Screenshot hasil pengujian serangan *spoofing* protokol EIGRP dengan *bandwidth* 50M.

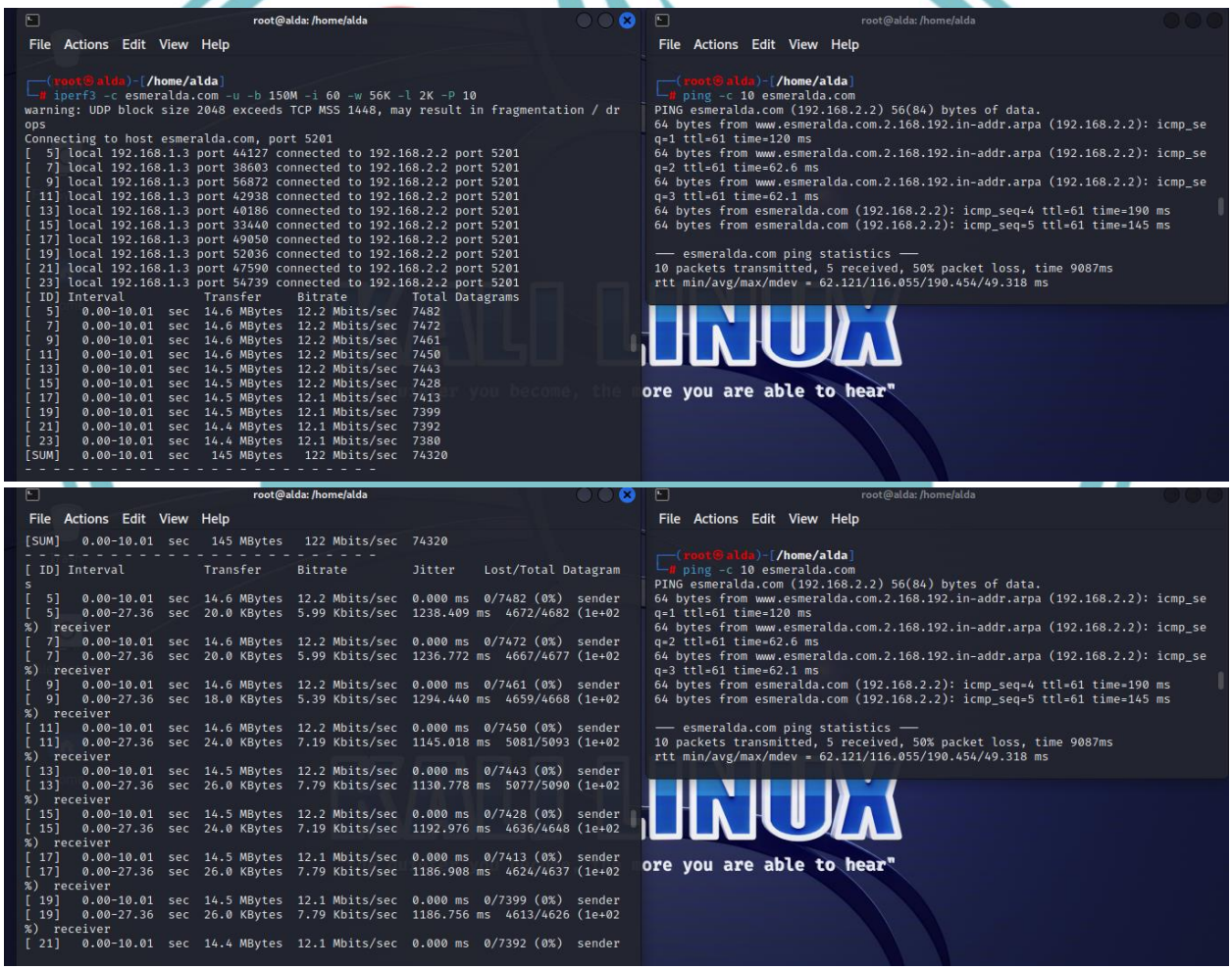


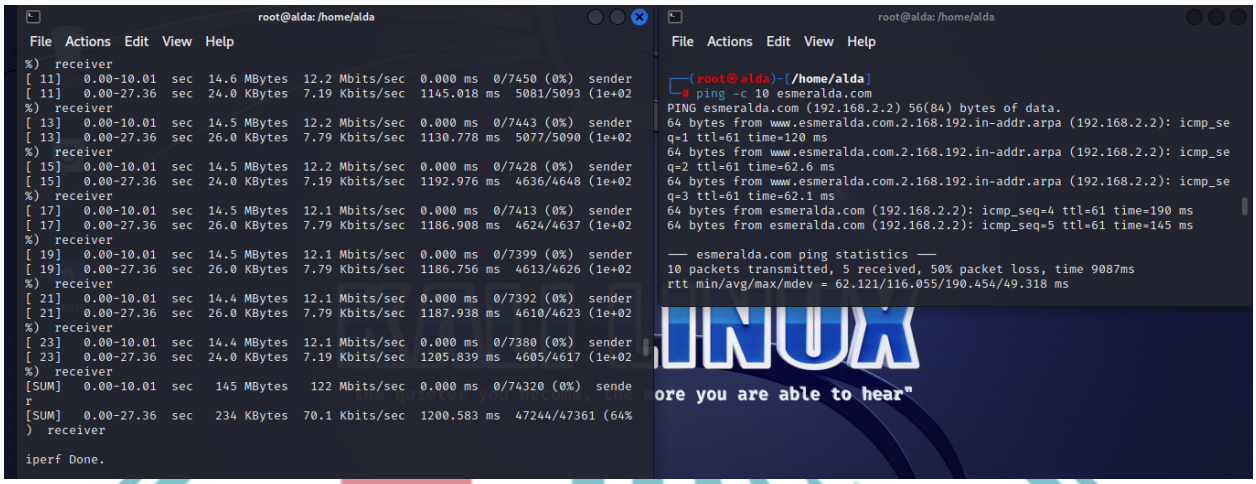
Screenshot hasil pengujian serangan *spoofing* protokol EIGRP dengan *bandwidth* 100M.

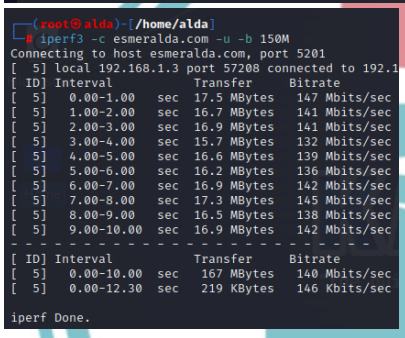


```
┌──(root㉿alda)-[/home/alda]
└─# iperf3 -c esmeralda.com -u -b 100M
Connecting to host esmeralda.com, port 5201
[  5] local 192.168.1.3 port 55213 connected to 192.16
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-1.00   sec  11.9 MBytes  99.3 Mbits/sec
[  5]   1.00-2.00   sec  12.0 MBytes   101 Mbits/sec
[  5]   2.00-3.00   sec  11.9 MBytes   100 Mbits/sec
[  5]   3.00-4.00   sec  11.9 MBytes   100 Mbits/sec
[  5]   4.00-5.00   sec  11.9 MBytes  99.9 Mbits/sec
[  5]   5.00-6.00   sec  11.7 MBytes  98.2 Mbits/sec
[  5]   6.00-7.00   sec  12.1 MBytes   102 Mbits/sec
[  5]   7.00-8.00   sec  11.9 MBytes   100 Mbits/sec
[  5]   8.00-9.00   sec  11.9 MBytes   100 Mbits/sec
[  5]   9.00-10.00  sec  11.9 MBytes   100 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-10.00  sec   119 MBytes   100 Mbits/sec
[  5]   0.00-27.53  sec   296 KBytes  87.9 Kbits/sec

iperf Done.
```

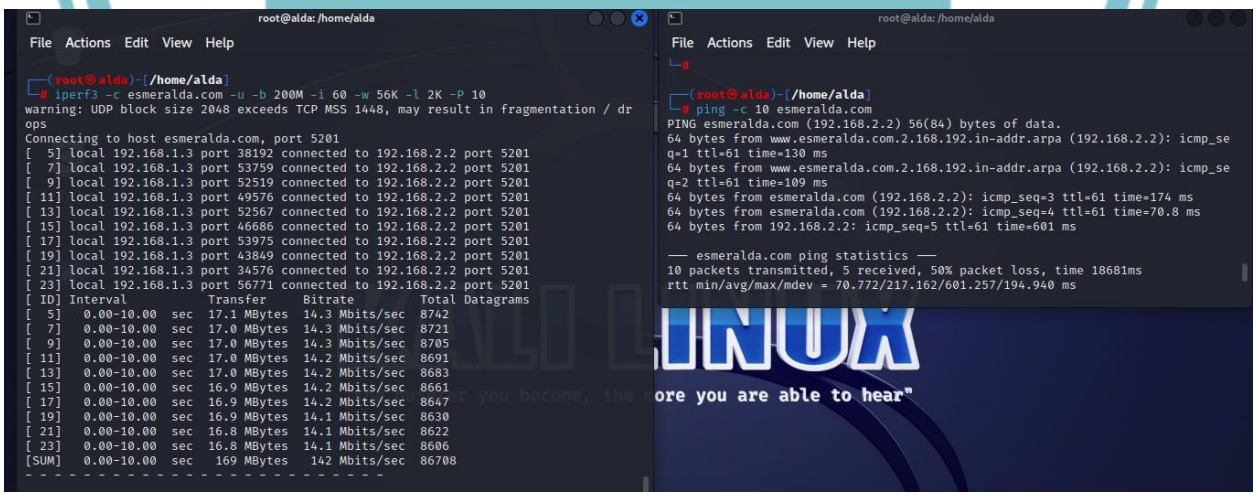
Screenshot hasil pengujian serangan *spoofing* protokol EIGRP dengan *bandwidth* 150M.





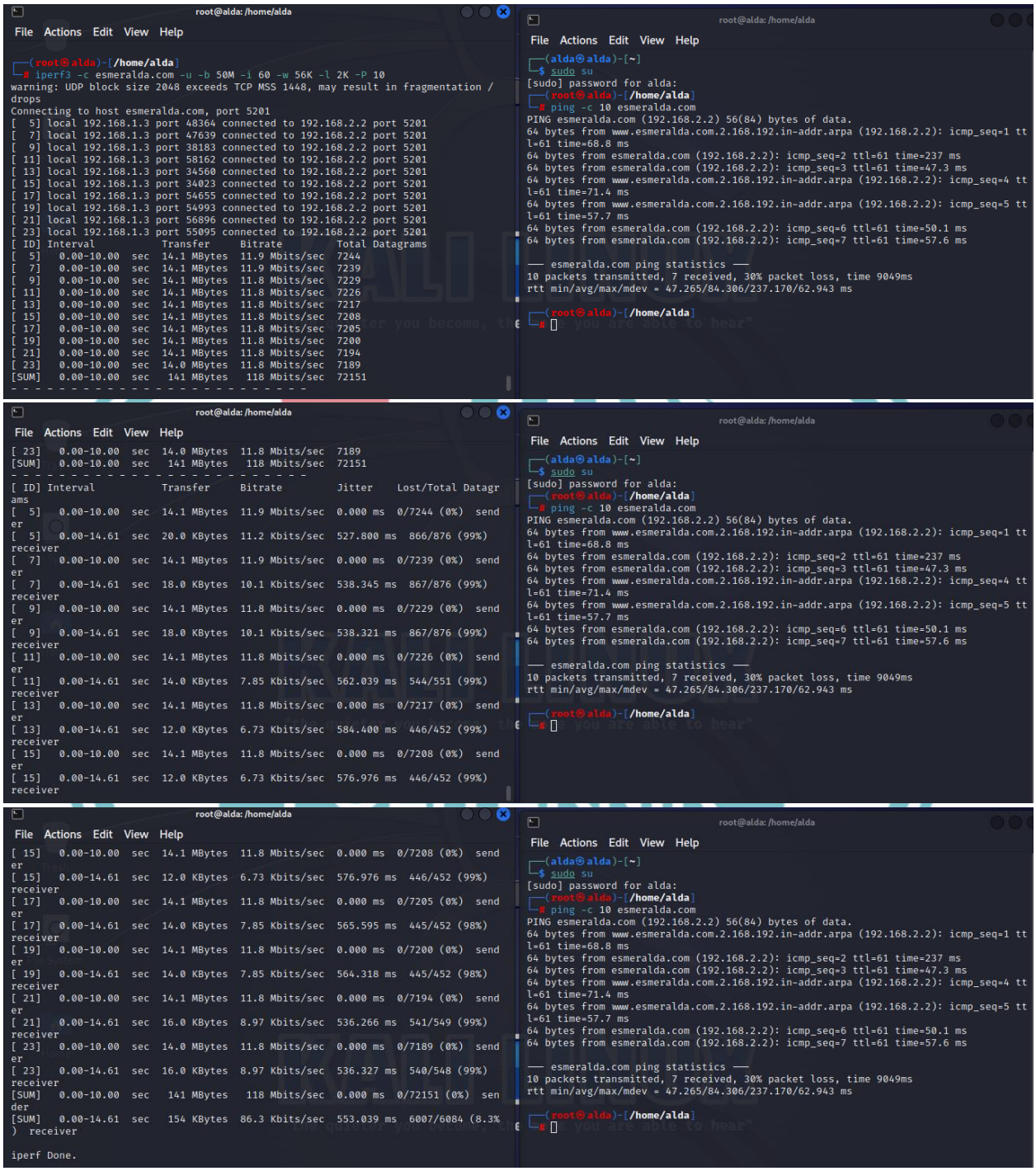


Screenshot hasil pengujian serangan *spoofing* protokol EIGRP dengan *bandwidth* 200M.



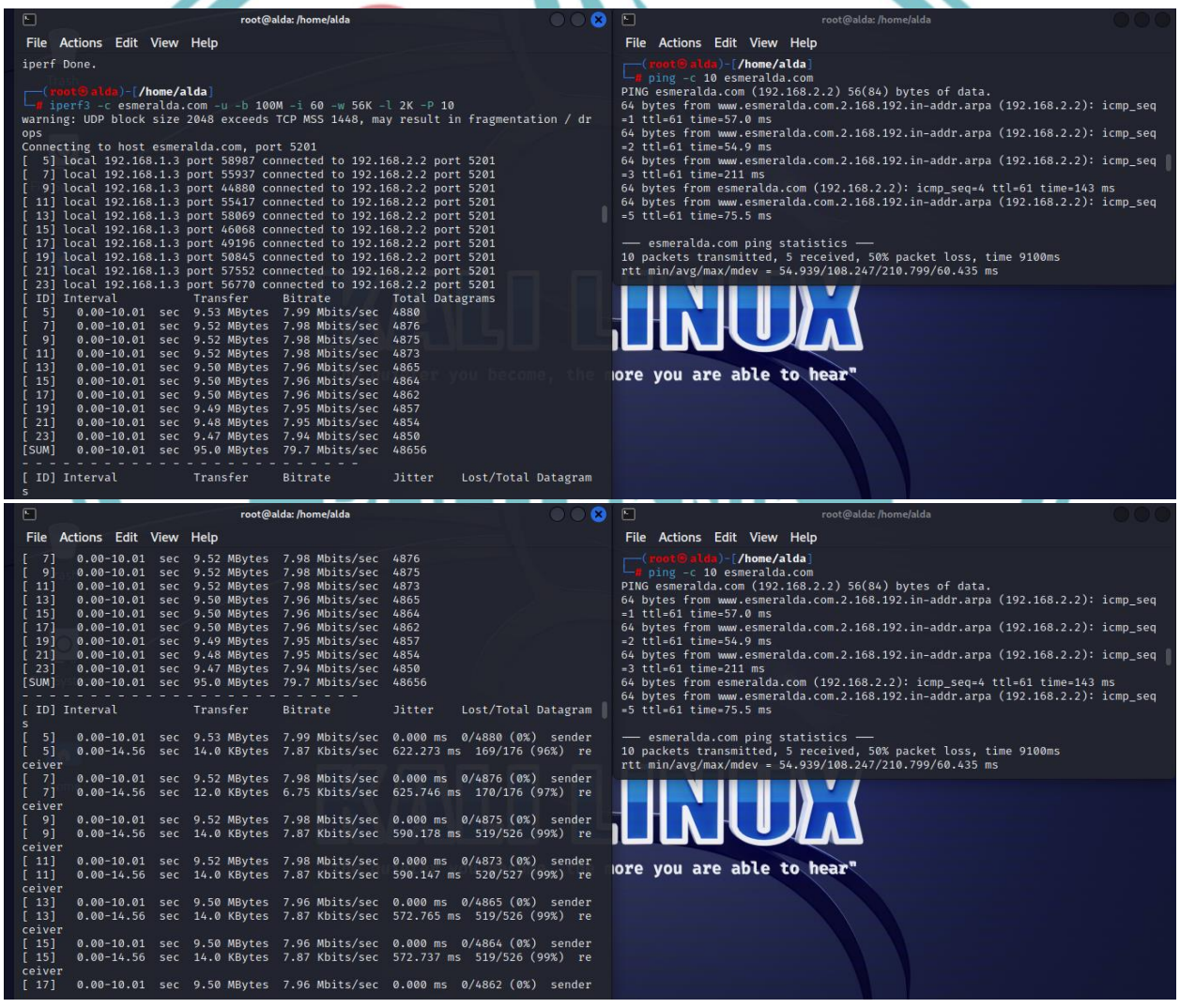
Screenshot hasil pengujian serangan *sniffing* protokol EIGRP dengan *bandwidth* 1K.

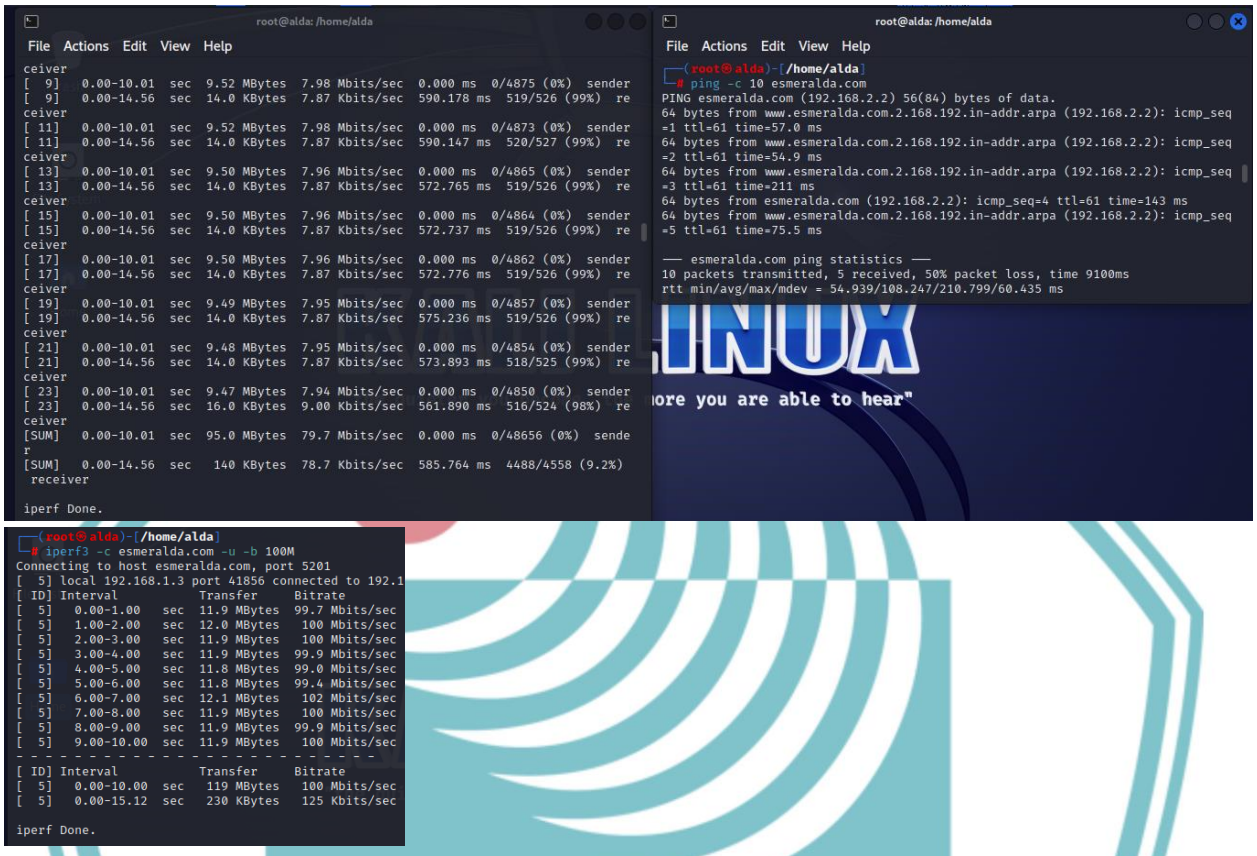
Screenshot hasil pengujian serangan *sniffing* protokol EIGRP dengan *bandwidth* 50M.



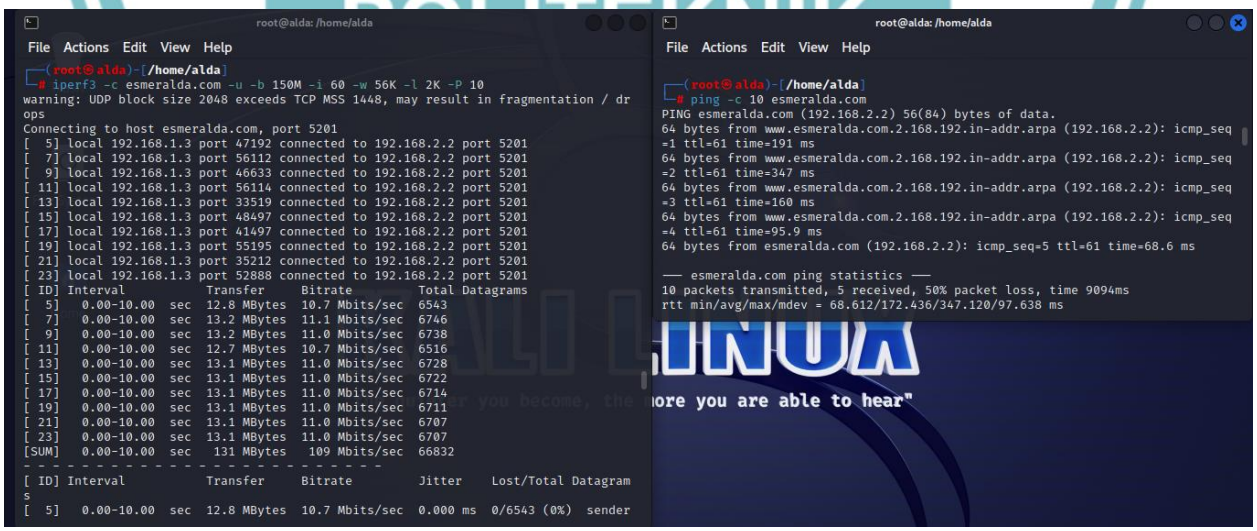
```
┌──(root㉿alda)-[/home/alda]
└─# iperf3 -c esmeralda.com -u -b 50M
Connecting to host esmeralda.com, port 5201
[  5] local 192.168.1.3 port 53652 connected to 192.16
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-1.00   sec  5.96 MBytes  50.0 Mbits/sec
[  5]   1.00-2.00   sec  5.96 MBytes  50.0 Mbits/sec
[  5]   2.00-3.00   sec  5.94 MBytes  49.8 Mbits/sec
[  5]   3.00-4.00   sec  5.98 MBytes  50.1 Mbits/sec
[  5]   4.00-5.00   sec  5.96 MBytes  50.0 Mbits/sec
[  5]   5.00-6.00   sec  5.96 MBytes  50.0 Mbits/sec
[  5]   6.00-7.00   sec  5.96 MBytes  50.0 Mbits/sec
[  5]   7.00-8.00   sec  5.96 MBytes  50.0 Mbits/sec
[  5]   8.00-9.00   sec  5.96 MBytes  50.0 Mbits/sec
[  5]   9.00-10.00  sec  5.96 MBytes  50.0 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-10.00  sec  59.6 MBytes  50.0 Mbits/sec
[  5]   0.00-18.90  sec   370 KBytes   161 Kbits/sec

iperf Done.
```

Screenshot hasil pengujian serangan *sniffing* protokol EIGRP dengan *bandwidth* 100M.

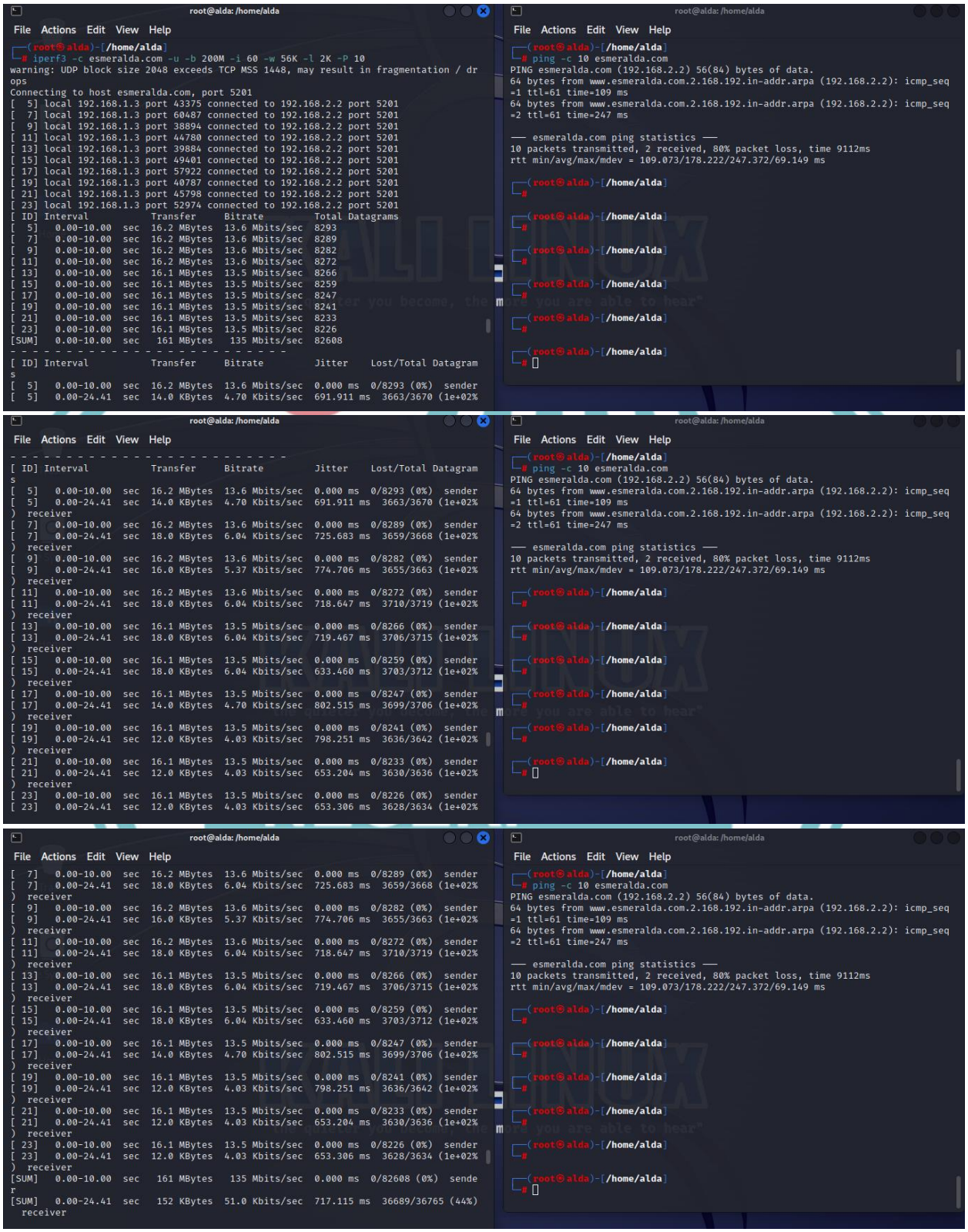




Screenshot hasil pengujian serangan *sniffing* protokol EIGRP dengan *bandwidth* 150M.

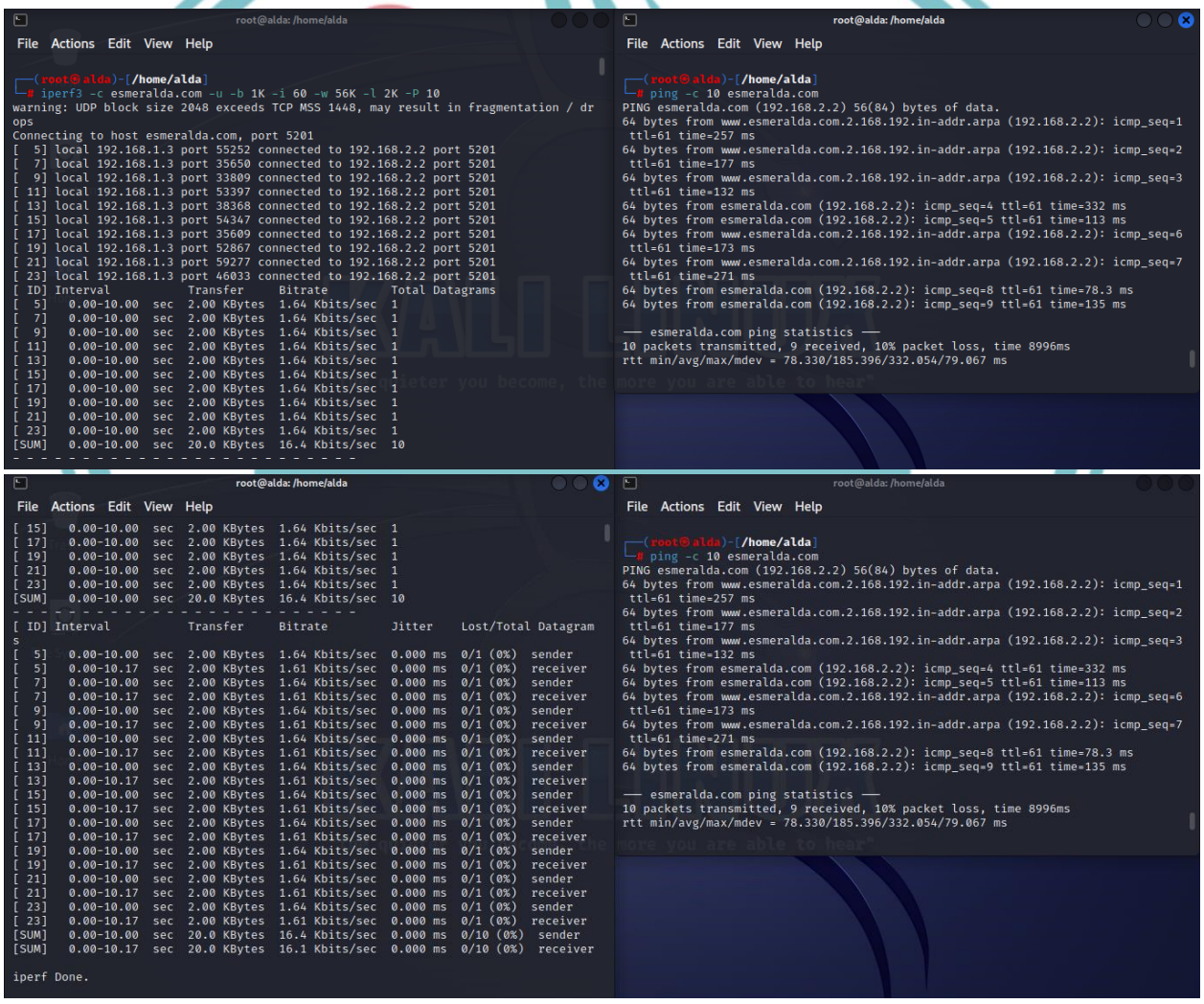


Screenshot hasil pengujian serangan *sniffing* protokol EIGRP dengan *bandwidth* 200M.



```
┌──(root㉿alda)-[/home/alda]
└─# iperf3 -c esmeralda.com -u -b 200M
Connecting to host esmeralda.com, port 5201
[  5] local 192.168.1.3 port 60959 connected to 192.1
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-1.00   sec  16.3 MBytes   137 Mbits/sec
[  5]   1.00-2.00   sec  17.3 MBytes   145 Mbits/sec
[  5]   2.00-3.00   sec  16.6 MBytes   140 Mbits/sec
[  5]   3.00-4.00   sec  17.2 MBytes   144 Mbits/sec
[  5]   4.00-5.00   sec  16.8 MBytes   141 Mbits/sec
[  5]   5.00-6.00   sec  16.1 MBytes   135 Mbits/sec
[  5]   6.00-7.00   sec  17.0 MBytes   143 Mbits/sec
[  5]   7.00-8.00   sec  16.5 MBytes   139 Mbits/sec
[  5]   8.00-9.00   sec  16.6 MBytes   140 Mbits/sec
[  5]   9.00-10.00  sec  17.2 MBytes   144 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-10.00  sec   168 MBytes   141 Mbits/sec
[  5]   0.00-19.50  sec   206 KBytes  86.7 Kbits/sec

iperf Done.
```

Screenshot hasil pengujian serangan *spoofing* dan *sniffing* protokol EIGRP dengan *bandwidth* 1K.



```
┌──(root㉿alda)-[/home/alda]
└─# iperf3 -c esmeralda.com -u -b 1K
Connecting to host esmeralda.com, port 5201
[  5] local 192.168.1.3 port 38803 connected to 192.
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-1.00   sec  1.41 KBytes  11.6 Kbits/sec
[  5]   1.00-2.00   sec  0.00 Bytes  0.00 bits/sec
[  5]   2.00-3.00   sec  0.00 Bytes  0.00 bits/sec
[  5]   3.00-4.00   sec  0.00 Bytes  0.00 bits/sec
[  5]   4.00-5.00   sec  0.00 Bytes  0.00 bits/sec
[  5]   5.00-6.00   sec  0.00 Bytes  0.00 bits/sec
[  5]   6.00-7.00   sec  0.00 Bytes  0.00 bits/sec
[  5]   7.00-8.00   sec  0.00 Bytes  0.00 bits/sec
[  5]   8.00-9.00   sec  0.00 Bytes  0.00 bits/sec
[  5]   9.00-10.00  sec  0.00 Bytes  0.00 bits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-10.00  sec  1.41 KBytes  1.16 Kbits/sec
[  5]   0.00-10.10  sec  1.41 KBytes  1.15 Kbits/sec

iperf Done.
```

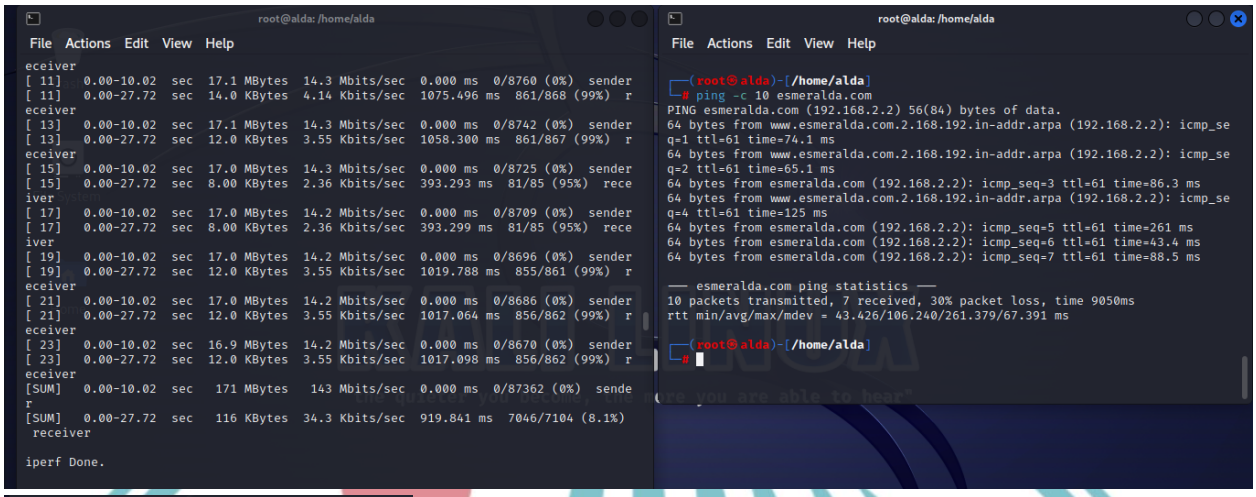
Screenshot hasil pengujian serangan *spoofing* dan *sniffing* protokol EIGRP dengan *bandwidth* 50M.

```
root@alda: /home/alda
File  Actions  Edit  View  Help

┌──(root㉿alda)-[/home/alda]
└─# iperf3 -c esmeralda.com -u -b 50M -i 60 -w 56K -l 2K -P 10
warning: UDP block size 2048 exceeds TCP MSS 1448, may result in fragmentation / dr
ops
Connecting to host esmeralda.com, port 5201
[  5] local 192.168.1.3 port 37581 connected to 192.168.2.2 port 5201
[  7] local 192.168.1.3 port 50602 connected to 192.168.2.2 port 5201
[  9] local 192.168.1.3 port 44178 connected to 192.168.2.2 port 5201
[ 11] local 192.168.1.3 port 45727 connected to 192.168.2.2 port 5201
[ 13] local 192.168.1.3 port 36145 connected to 192.168.2.2 port 5201
[ 15] local 192.168.1.3 port 56690 connected to 192.168.2.2 port 5201
[ 17] local 192.168.1.3 port 60845 connected to 192.168.2.2 port 5201
[ 19] local 192.168.1.3 port 56461 connected to 192.168.2.2 port 5201
[ 21] local 192.168.1.3 port 51648 connected to 192.168.2.2 port 5201
[ 23] local 192.168.1.3 port 48712 connected to 192.168.2.2 port 5201
[ ID] Interval           Transfer     Bitrate         Total Datagrams
[  5]   0.00-10.02  sec  17.2 MBytes  14.4 Mbits/sec  8804
[  7]   0.00-10.02  sec  17.2 MBytes  14.4 Mbits/sec  8789
[  9]   0.00-10.02  sec  17.2 MBytes  14.4 Mbits/sec  8781
[ 11]   0.00-10.02  sec  17.1 MBytes  14.3 Mbits/sec  8760
[ 13]   0.00-10.02  sec  17.1 MBytes  14.3 Mbits/sec  8742
[ 15]   0.00-10.02  sec  17.0 MBytes  14.3 Mbits/sec  8725
[ 17]   0.00-10.02  sec  17.0 MBytes  14.2 Mbits/sec  8709
[ 19]   0.00-10.02  sec  17.0 MBytes  14.2 Mbits/sec  8696
[ 21]   0.00-10.02  sec  17.0 MBytes  14.2 Mbits/sec  8686
[ 23]   0.00-10.02  sec  16.9 MBytes  14.2 Mbits/sec  8670
[SUM]   0.00-10.02  sec   171 MBytes   143 Mbits/sec  87362
- - - - - - - - - - - - - - - - - - - - - - - - -
```

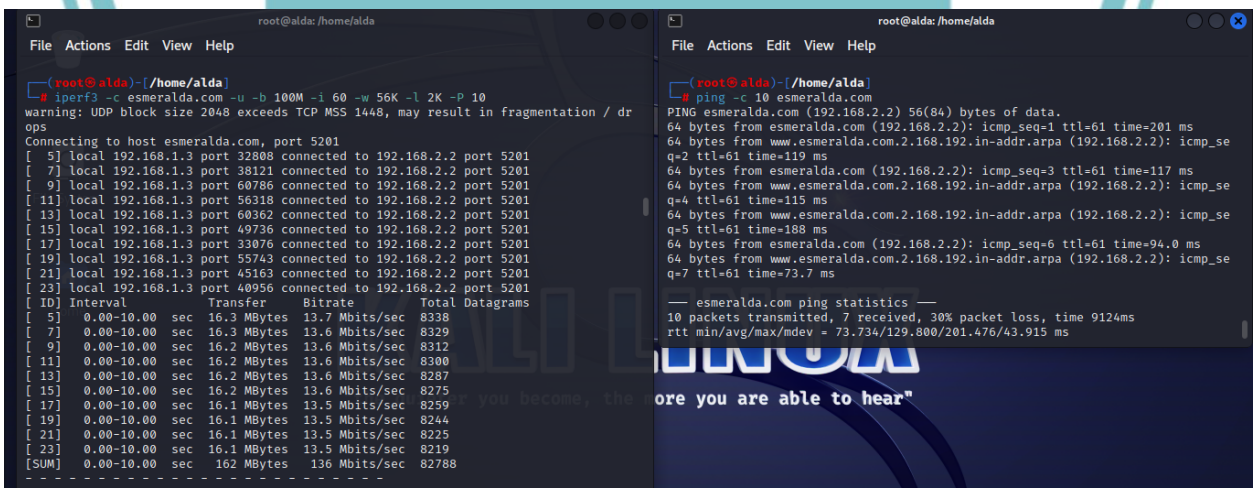
```
root@alda: /home/alda
File  Actions  Edit  View  Help

┌──(root㉿alda)-[/home/alda]
└─# ping -c 10 esmeralda.com
PING esmeralda.com (192.168.2.2) 56(84) bytes of data.
64 bytes from www.esmeralda.com.2.168.192.in-addr.arpa (192.168.2.2): icmp_se
q=1 ttl=61 time=74.1 ms
64 bytes from www.esmeralda.com.2.168.192.in-addr.arpa (192.168.2.2): icmp_se
q=2 ttl=61 time=65.1 ms
64 bytes from esmeralda.com (192.168.2.2): icmp_seq=3 ttl=61 time=86.3 ms
64 bytes from www.esmeralda.com.2.168.192.in-addr.arpa (192.168.2.2): icmp_se
q=4 ttl=61 time=125 ms
64 bytes from esmeralda.com (192.168.2.2): icmp_seq=5 ttl=61 time=261 ms
64 bytes from esmeralda.com (192.168.2.2): icmp_seq=6 ttl=61 time=43.4 ms
64 bytes from esmeralda.com (192.168.2.2): icmp_seq=7 ttl=61 time=88.5 ms

── esmeralda.com ping statistics ──
10 packets transmitted, 7 received, 30% packet loss, time 9050ms
rtt min/avg/max/mdev = 43.426/106.240/261.379/67.391 ms

┌──(root㉿alda)-[/home/alda]
└─#
```

```
root@alda: /home/alda
File  Actions  Edit  View  Help

[SUM]   0.00-10.02  sec   171 MBytes   143 Mbits/sec  87362
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datagram
s
[  5]   0.00-10.02  sec  17.2 MBytes  14.4 Mbits/sec  0.000 ms  0/8804 (0%)  sender
[  5]   0.00-27.72  sec  14.0 KBytes  4.14 Kbits/sec  1057.858 ms  866/873 (99%)  r
eceiver
[  7]   0.00-10.02  sec  17.2 MBytes  14.4 Mbits/sec  0.000 ms  0/8789 (0%)  sender
[  7]   0.00-27.72  sec  10.0 KBytes  2.96 Kbits/sec  1088.658 ms  867/872 (99%)  r
eceiver
[  9]   0.00-10.02  sec  17.2 MBytes  14.4 Mbits/sec  0.000 ms  0/8781 (0%)  sender
[  9]   0.00-27.72  sec  14.0 KBytes  4.14 Kbits/sec  1077.555 ms  862/869 (99%)  r
eceiver
[ 11]   0.00-10.02  sec  17.1 MBytes  14.3 Mbits/sec  0.000 ms  0/8760 (0%)  sender
[ 11]   0.00-27.72  sec  14.0 KBytes  4.14 Kbits/sec  1075.496 ms  861/868 (99%)  r
eceiver
[ 13]   0.00-10.02  sec  17.1 MBytes  14.3 Mbits/sec  0.000 ms  0/8742 (0%)  sender
[ 13]   0.00-27.72  sec  12.0 KBytes  3.55 Kbits/sec  1058.300 ms  861/867 (99%)  r
eceiver
[ 15]   0.00-10.02  sec  17.0 MBytes  14.3 Mbits/sec  0.000 ms  0/8725 (0%)  sender
[ 15]   0.00-27.72  sec  8.00 KBytes  2.36 Kbits/sec  393.293 ms  81/85 (95%)  rece
iver
[ 17]   0.00-10.02  sec  17.0 MBytes  14.2 Mbits/sec  0.000 ms  0/8709 (0%)  sender
[ 17]   0.00-27.72  sec  8.00 KBytes  2.36 Kbits/sec  393.299 ms  81/85 (95%)  rece
iver
[ 19]   0.00-10.02  sec  17.0 MBytes  14.2 Mbits/sec  0.000 ms  0/8696 (0%)  sender
[ 19]   0.00-27.72  sec  12.0 KBytes  3.55 Kbits/sec  1019.788 ms  855/861 (99%)  r
eceiver
[ 21]   0.00-10.02  sec  17.0 MBytes  14.2 Mbits/sec  0.000 ms  0/8686 (0%)  sender
```

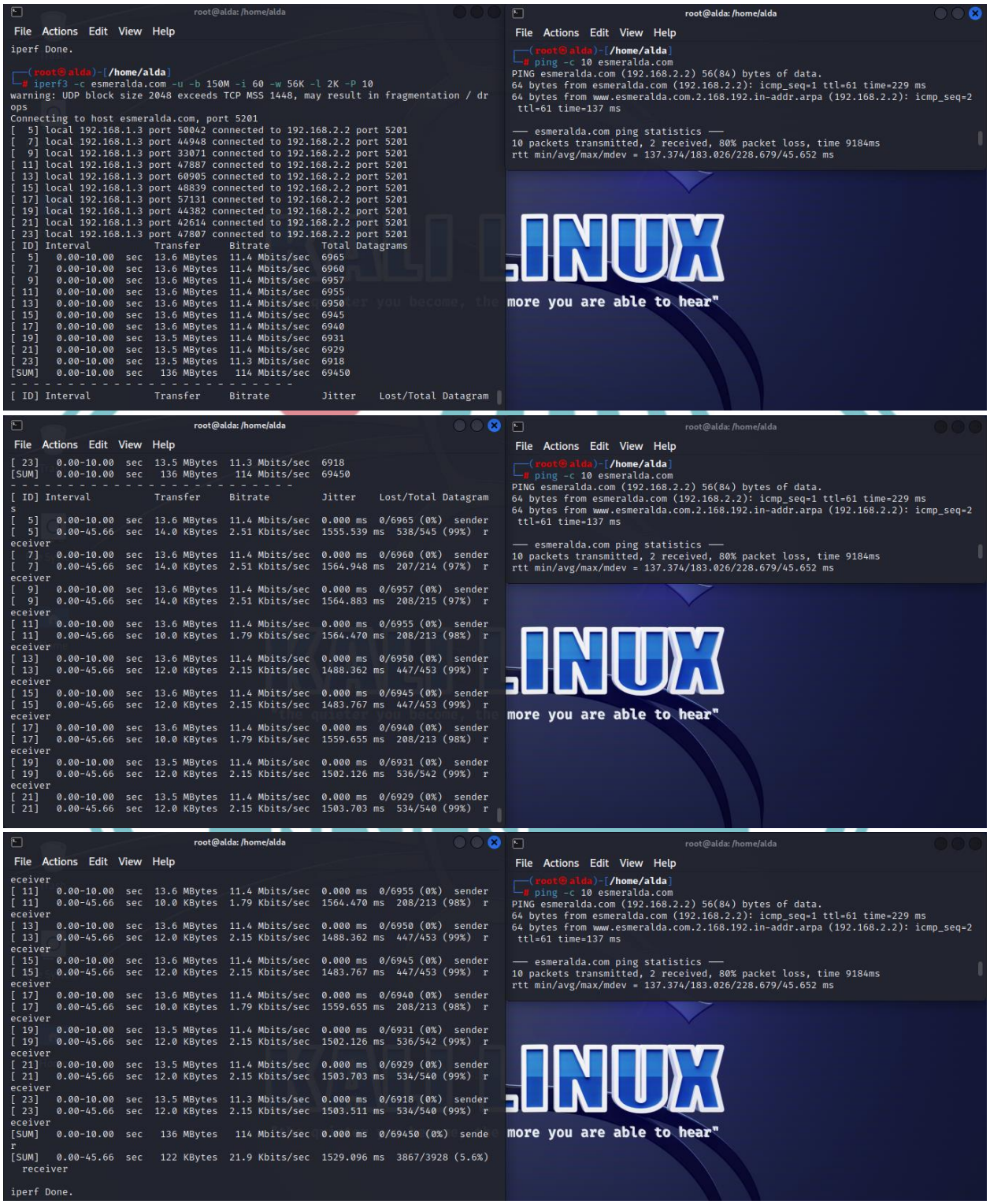
```
root@alda: /home/alda
File  Actions  Edit  View  Help

┌──(root㉿alda)-[/home/alda]
└─# ping -c 10 esmeralda.com
PING esmeralda.com (192.168.2.2) 56(84) bytes of data.
64 bytes from www.esmeralda.com.2.168.192.in-addr.arpa (192.168.2.2): icmp_se
q=1 ttl=61 time=74.1 ms
64 bytes from www.esmeralda.com.2.168.192.in-addr.arpa (192.168.2.2): icmp_se
q=2 ttl=61 time=65.1 ms
64 bytes from esmeralda.com (192.168.2.2): icmp_seq=3 ttl=61 time=86.3 ms
64 bytes from www.esmeralda.com.2.168.192.in-addr.arpa (192.168.2.2): icmp_se
q=4 ttl=61 time=125 ms
64 bytes from esmeralda.com (192.168.2.2): icmp_seq=5 ttl=61 time=261 ms
64 bytes from esmeralda.com (192.168.2.2): icmp_seq=6 ttl=61 time=43.4 ms
64 bytes from esmeralda.com (192.168.2.2): icmp_seq=7 ttl=61 time=88.5 ms

── esmeralda.com ping statistics ──
10 packets transmitted, 7 received, 30% packet loss, time 9050ms
rtt min/avg/max/mdev = 43.426/106.240/261.379/67.391 ms

┌──(root㉿alda)-[/home/alda]
└─#
```



Screenshot hasil pengujian serangan *spoofing* dan *sniffing* protokol EIGRP dengan *bandwidth* 100M.

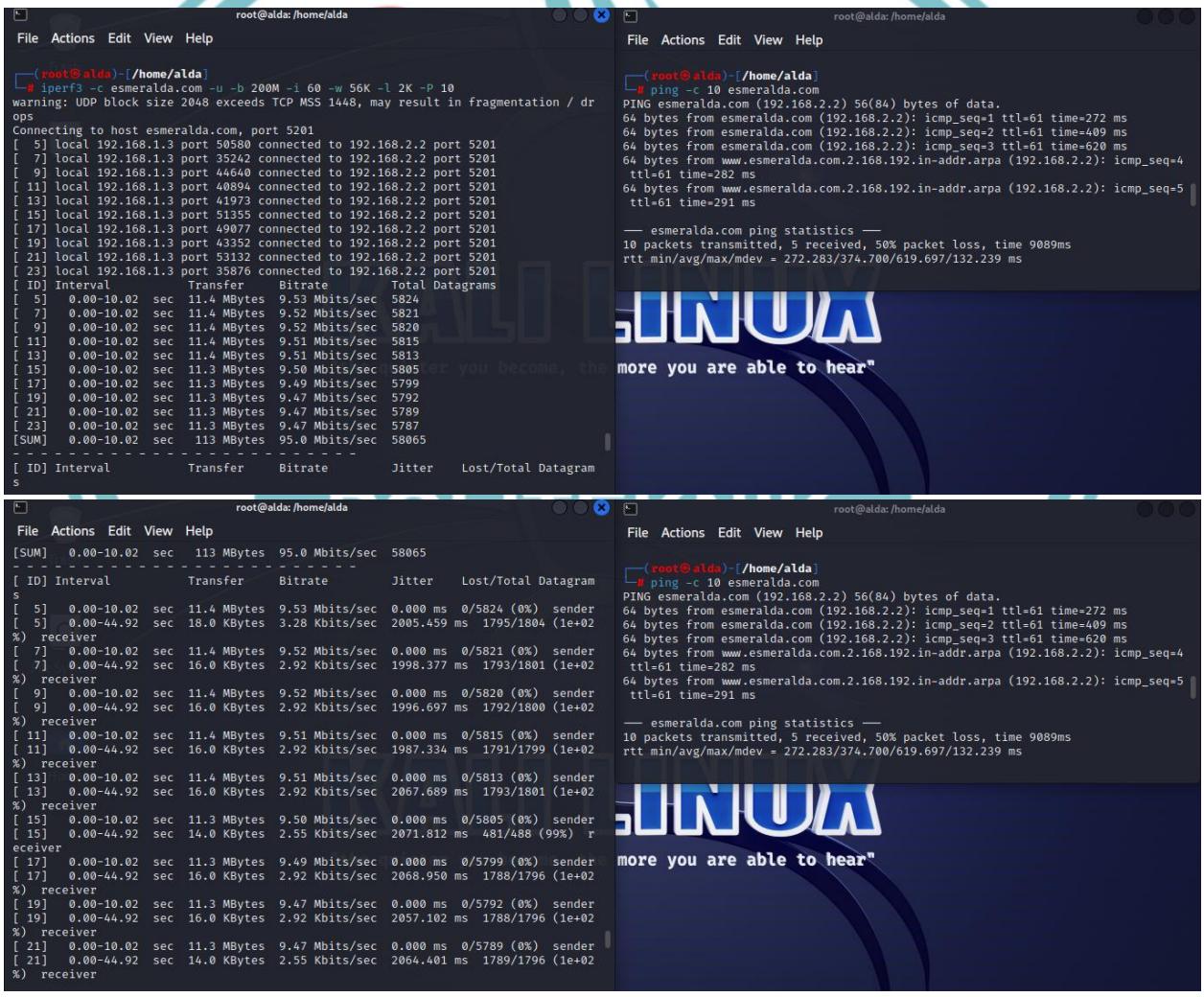


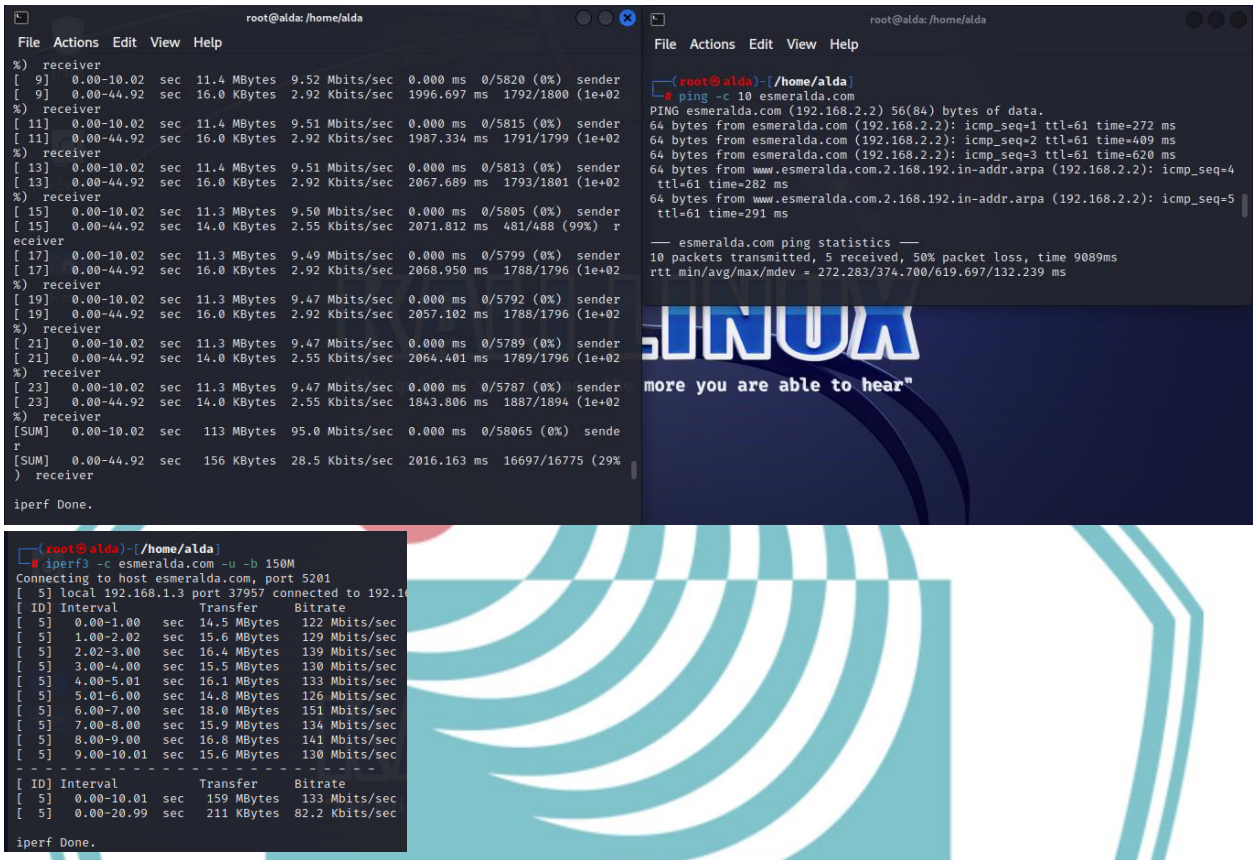
Screenshot hasil pengujian serangan *spoofing* dan *sniffing* protokol EIGRP dengan *bandwidth* 150M.



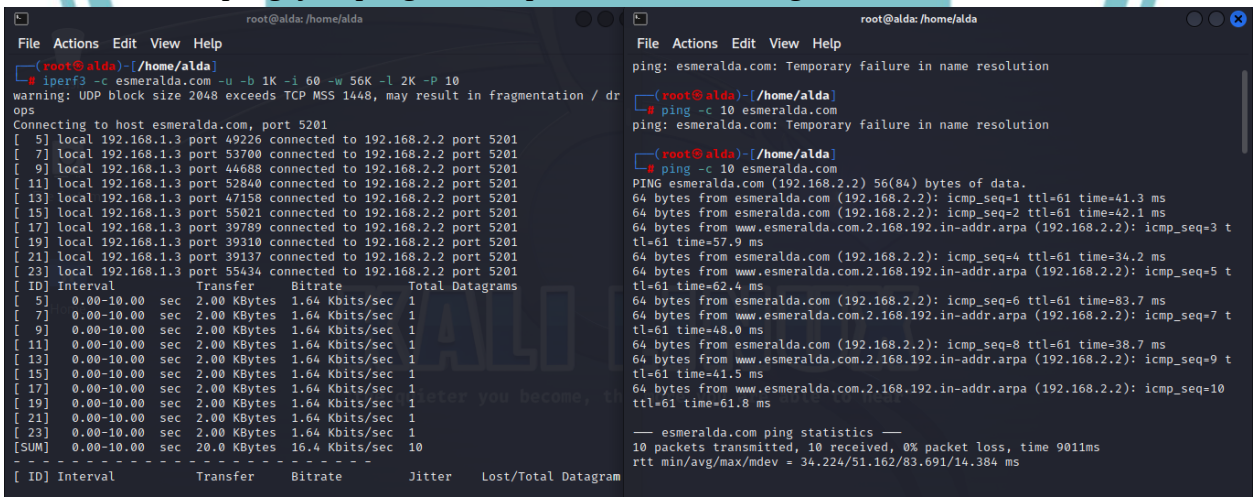
```
┌──(root㉿alda)-[/home/alda]
└─# iperf3 -c esmeralda.com -u -b 150M
Connecting to host esmeralda.com, port 5201
[  5] local 192.168.1.3 port 38410 connected to 192.1
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-1.00   sec  15.3 MBytes   128 Mbits/sec
[  5]   1.00-2.00   sec  16.5 MBytes   139 Mbits/sec
[  5]   2.00-3.00   sec  15.7 MBytes   132 Mbits/sec
[  5]   3.00-4.00   sec  17.1 MBytes   144 Mbits/sec
[  5]   4.00-5.00   sec  17.2 MBytes   144 Mbits/sec
[  5]   5.00-6.00   sec  17.3 MBytes   145 Mbits/sec
[  5]   6.00-7.00   sec  16.4 MBytes   137 Mbits/sec
[  5]   7.00-8.00   sec  16.3 MBytes   137 Mbits/sec
[  5]   8.00-9.00   sec  14.7 MBytes   123 Mbits/sec
[  5]   9.00-10.02  sec  15.6 MBytes   129 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-10.02  sec   162 MBytes   136 Mbits/sec
[  5]   0.00-27.79  sec   180 KBytes  52.9 Kbits/sec

iperf Done.
```

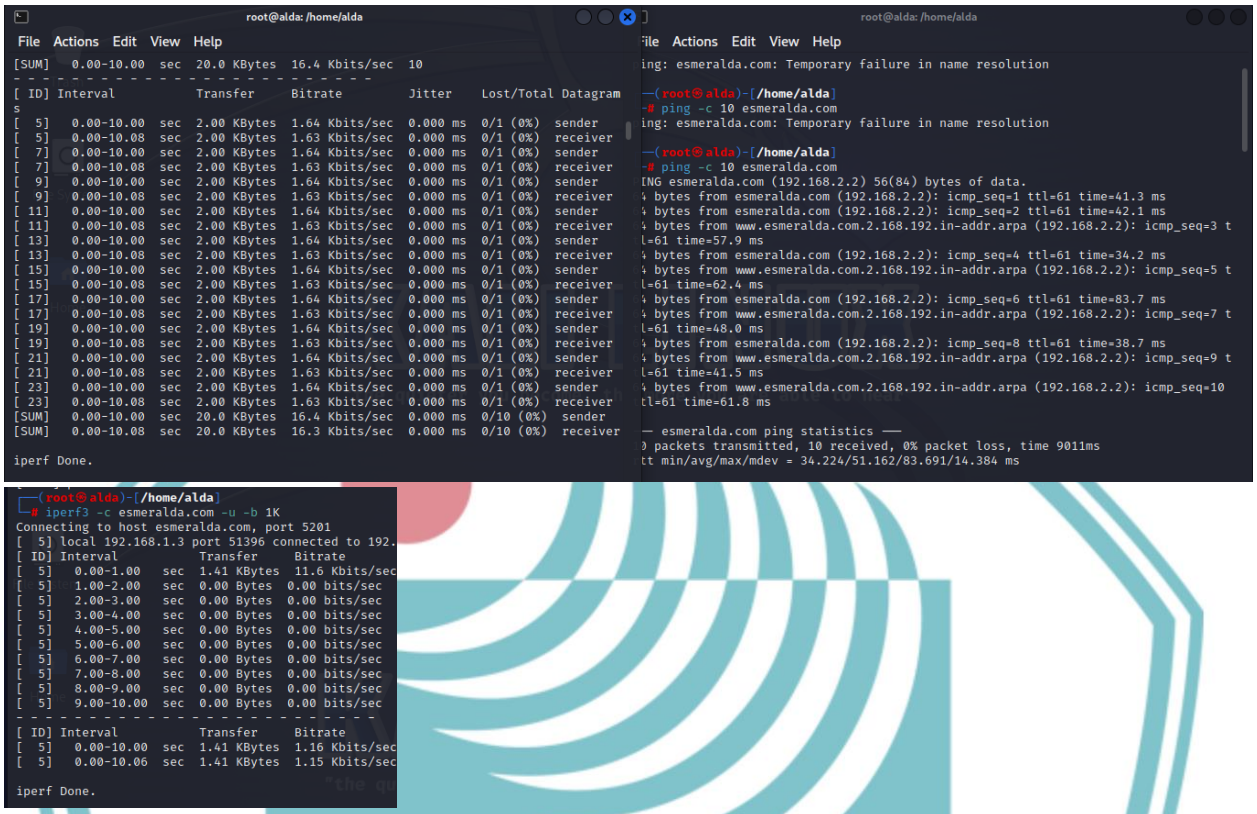
Screenshot hasil pengujian serangan *spoofing* dan *sniffing* protokol EIGRP dengan *bandwidth* 200M.



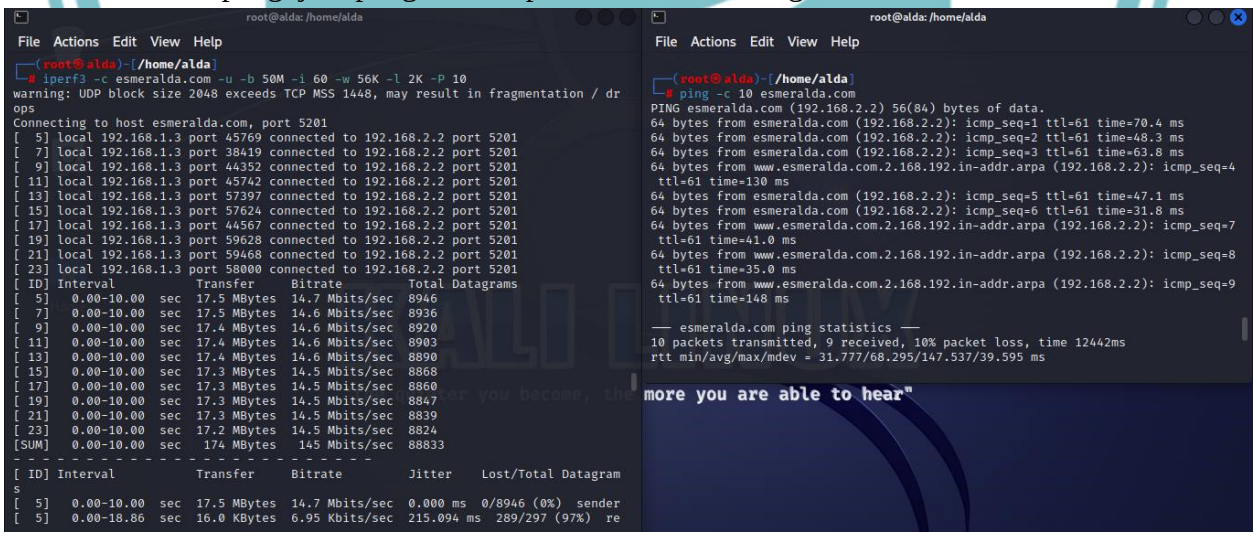


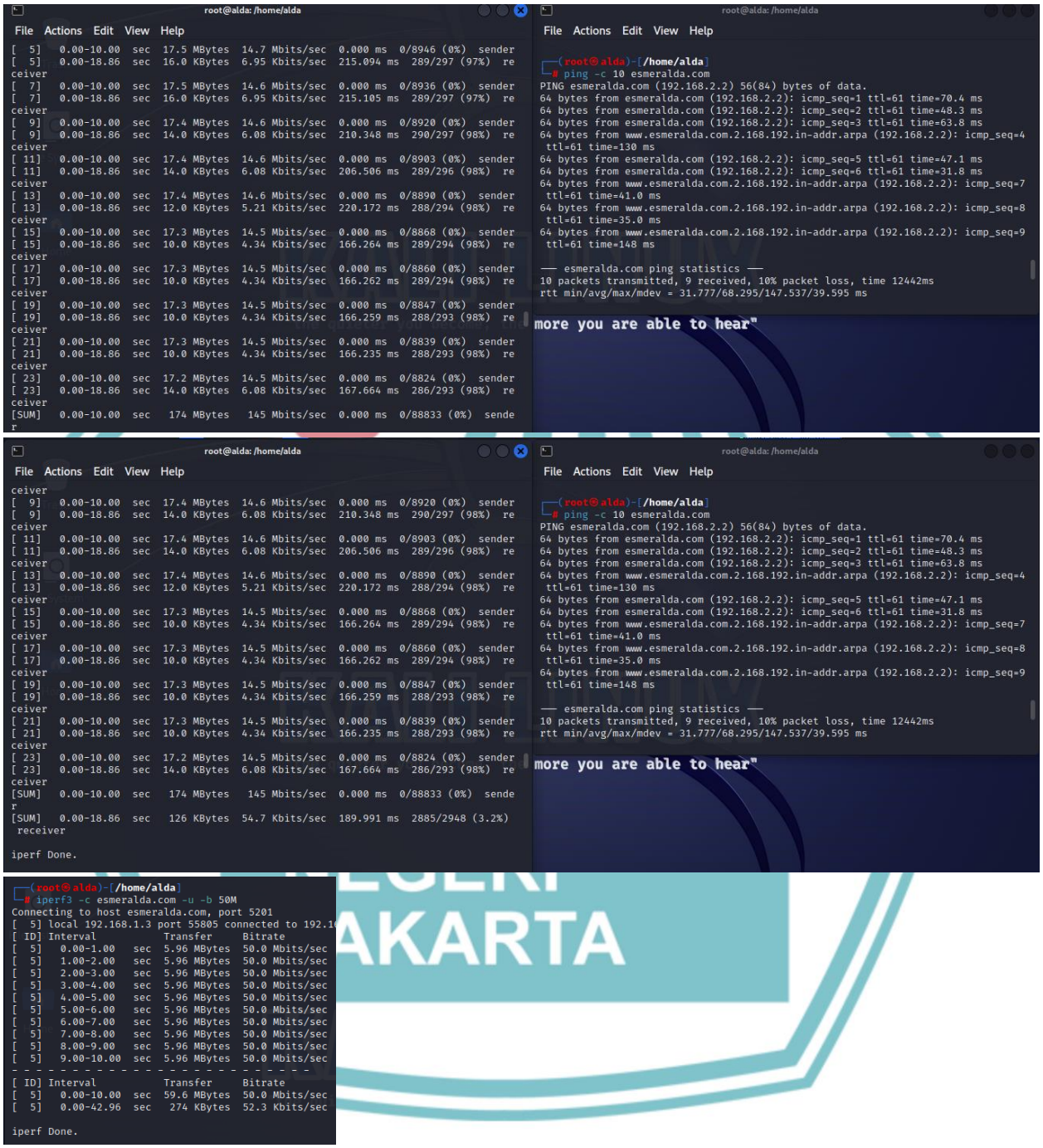
Screenshot hasil pengujian pengamanan protokol EIGRP dengan *bandwidth* 1K.



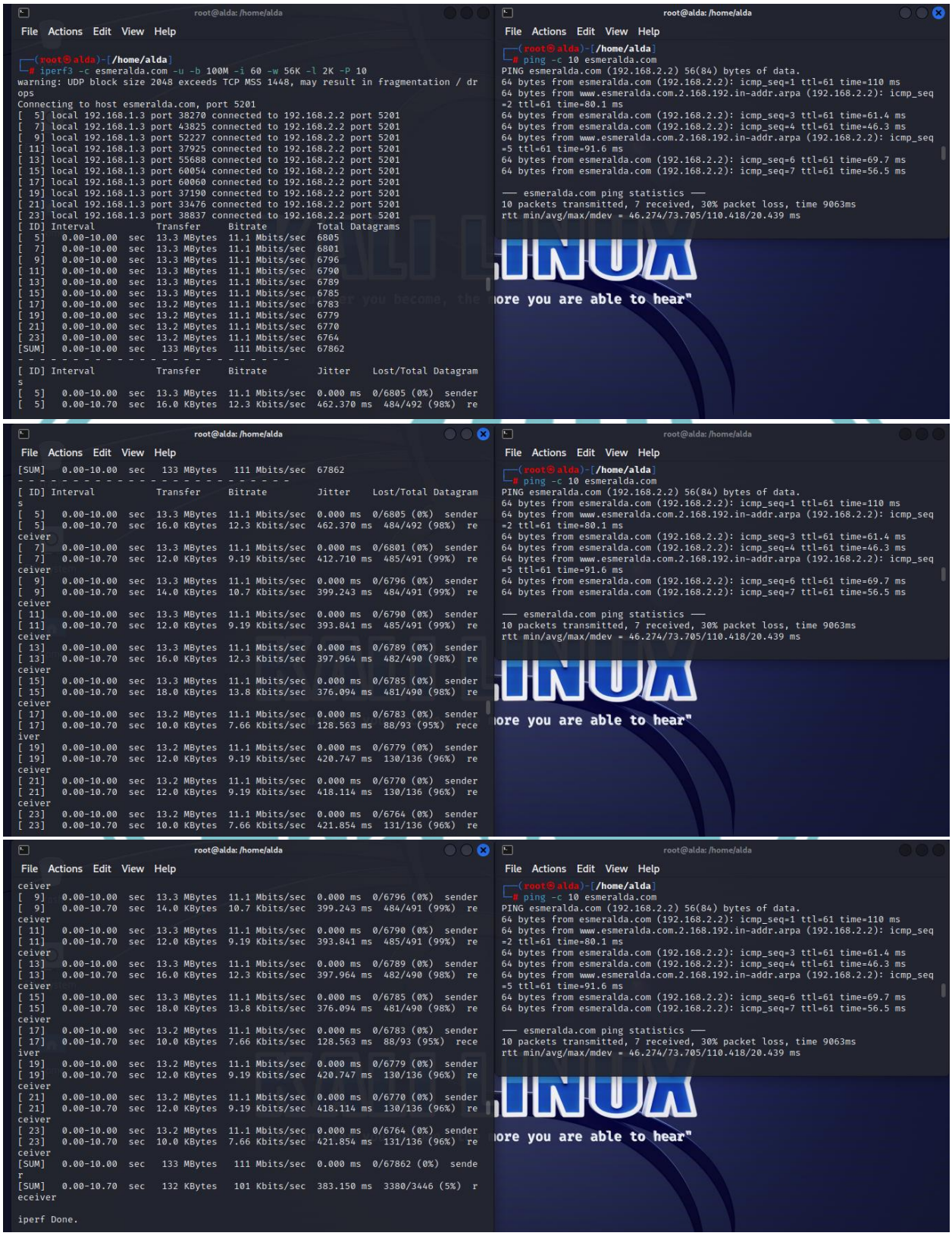


Screenshot hasil pengujian pengamanan protokol EIGRP dengan *bandwidth* 50M.



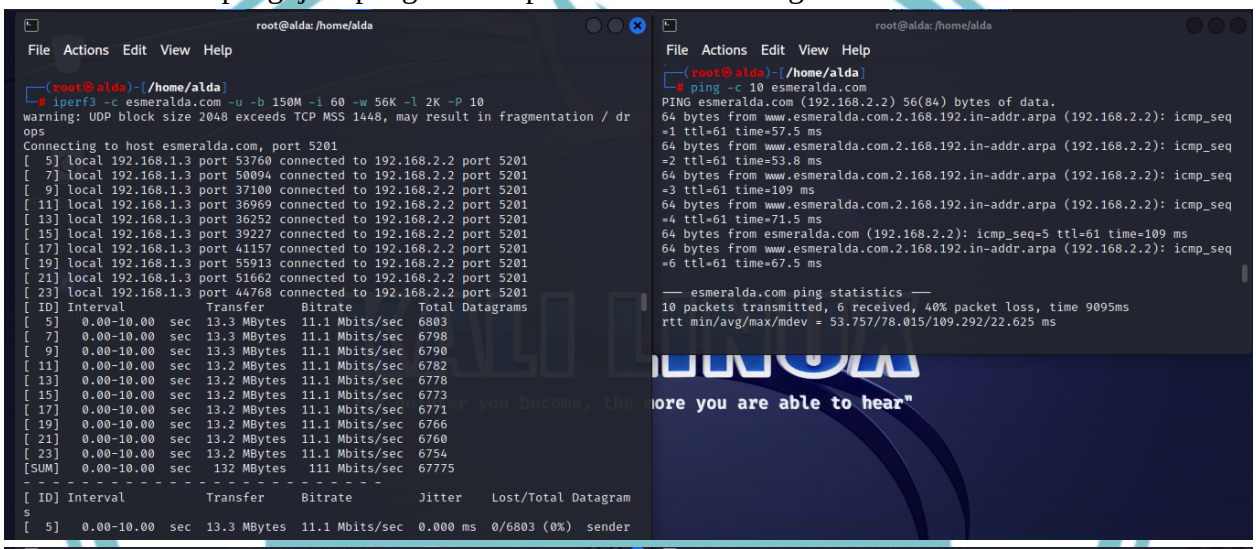


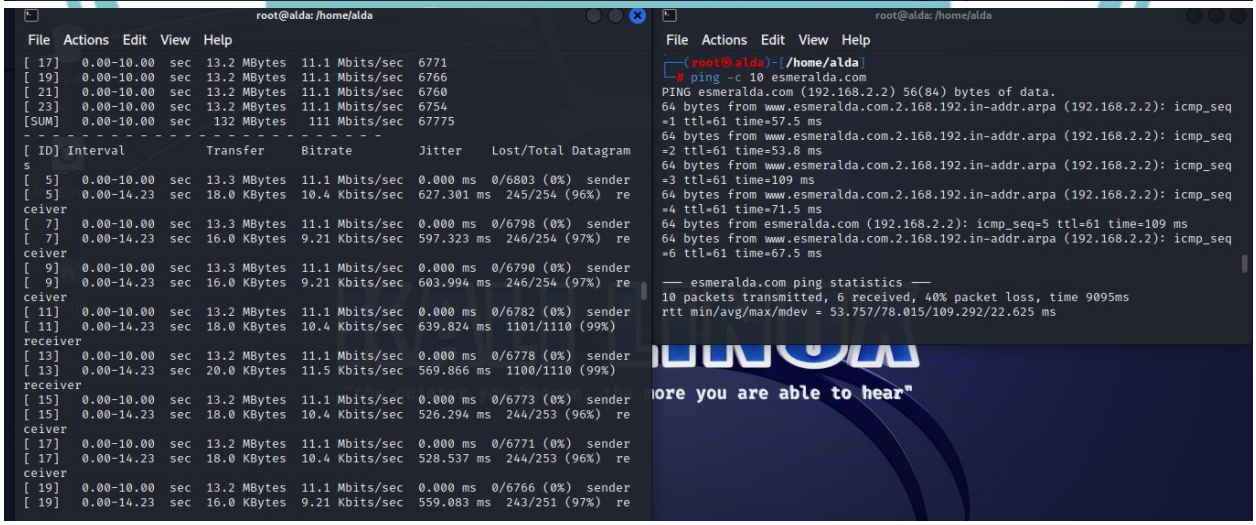
Screenshot hasil pengujian pengamanan protokol EIGRP dengan *bandwidth* 100M.

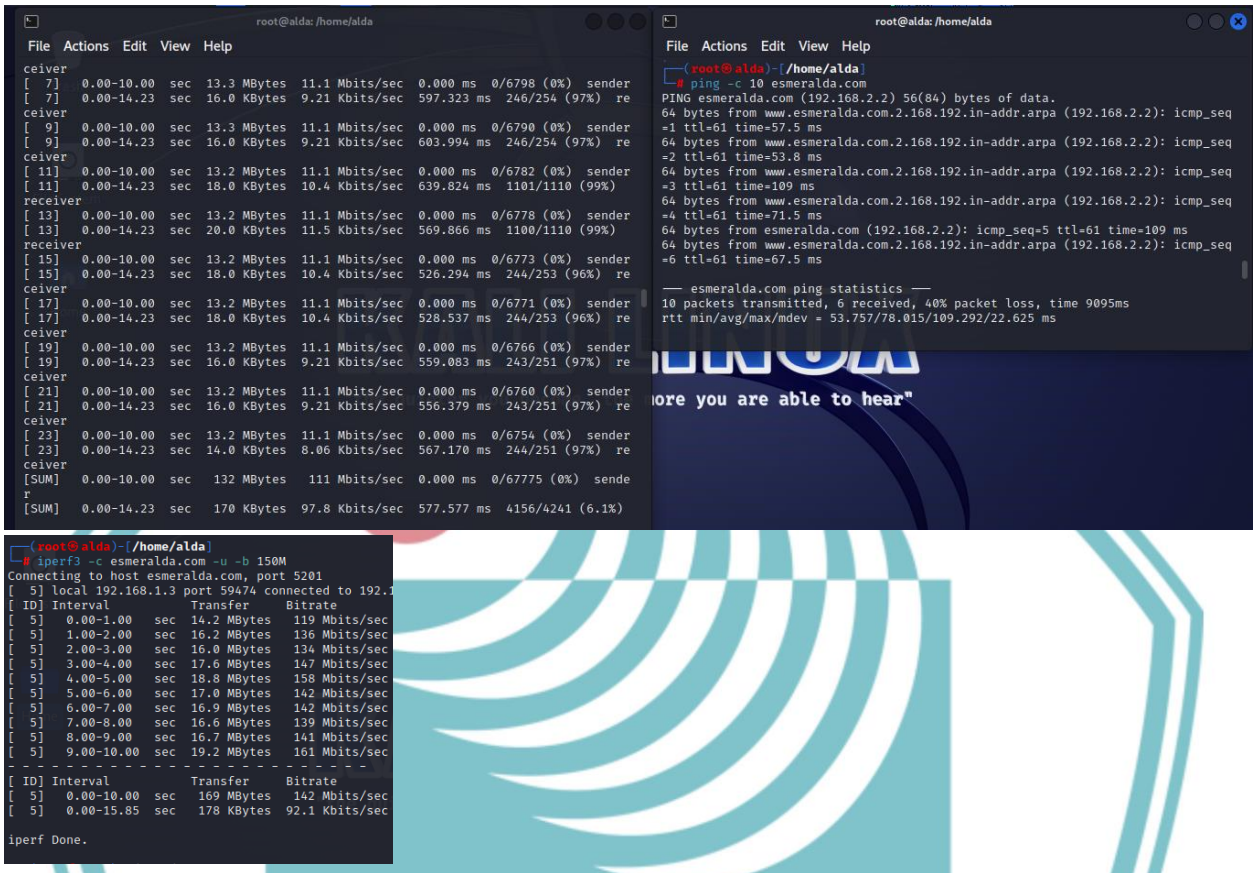


```
┌──(root㉿alda)-[/home/alda]
└─# iperf3 -c esmeralda.com -u -b 100M
Connecting to host esmeralda.com, port 5201
[  5] local 192.168.1.3 port 43765 connected to 192.1
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-1.00   sec  11.8 MBytes  99.4 Mbits/sec
[  5]   1.00-2.00   sec  12.0 MBytes   100 Mbits/sec
[  5]   2.00-3.00   sec  11.9 MBytes   100 Mbits/sec
[  5]   3.00-4.00   sec  11.9 MBytes  99.4 Mbits/sec
[  5]   4.00-5.00   sec  11.9 MBytes   100 Mbits/sec
[  5]   5.00-6.00   sec  12.0 MBytes   100 Mbits/sec
[  5]   6.00-7.00   sec  11.9 MBytes   100 Mbits/sec
[  5]   7.00-8.00   sec  11.9 MBytes   100 Mbits/sec
[  5]   8.00-9.00   sec  11.9 MBytes  99.9 Mbits/sec
[  5]   9.00-10.00  sec  11.9 MBytes   100 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-10.00  sec   119 MBytes   100 Mbits/sec
[  5]   0.00-25.92  sec   236 KBytes  74.6 Kbits/sec

iperf Done.
```

Screenshot hasil pengujian pengamanan protokol EIGRP dengan *bandwidth* 150M.







Screenshot hasil pengujian pengamanan protokol EIGRP dengan *bandwidth* 200M.