DAFTAR PUSTAKA

Al Mazari, A., Anjariny, A. H., Habib, S. A., & Nyakwende, E. (2018). Cyber terrorism taxonomies: Definition, targets, patterns, risk factors, and mitigation strategies. In Cyber security and threats: Concepts, methodologies, tools, and applications (pp. 608-621). IGI Global.

Chonka, A., & Abawajy, J. (2012, September). Detecting and mitigating HX-DoS attacks against cloud web services. In 2012 15th International Conference on Network-Based Information Systems (pp. 429-434). IEEE.

Diansyah, T. M., Faisal, I., & Siregar, D. (2023). Manajemen Pencegahan Serangan Jaringan Wireless Dari Serangan Man In The Middle Attack. *Kesatria: Jurnal Penerapan Sistem Informasi (Komputer dan Manajemen)*, *4*(1), 224-233.

EC-Council. (2020). Certified Network Defender (CND) Version 2. International Council of E-Commerce Consultants (EC Council).

Fahrina, Miftahul. (2023). Vulnerability Assessment Dalam Analisis Keamanan WLAN Departemen Teknik Elektro FT-UH. Universitas Hasanuddin

FIRST. (n.d.). CVSS v4.0 Specification Document. Forum of Incident Response and Security Teams. Retrieved December 13, 2023, from https://www.first.org/cvss/v4.0/specification-document

Gantsou, D. (2015). On the use of security analytics for attack detection in vehicular ad hoc networks. In 2015 international conference on cyber security of smart cities, industrial control system and communications (SSIC) (pp. 1-6). IEEE.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. International studies quarterly, 53(4), 1155-1175.

Haris, A. I., Riyanto, B., Surachman, F., & Ramadhan, A. A. (2022). Analisis Pengamanan Jaringan Menggunakan Router Mikrotik dari Serangan DoS dan Pengaruhnya Terhadap Performansi. Komputika: Jurnal Sistem Komputer, 11(1), 67-76.

Hesar, A. D., & Attari, M. A. (2014, December). Simulating and analysis of cyber attacks on a BLPC network. In 2014 Smart Grid Conference (SGC) (pp. 1-6). IEEE.

Hu, X., Jang, J., Stoecklin, M. P., Wang, T., Schales, D. L., Kirat, D., & Rao, J. R. (2016, June). BAYWATCH: robust beaconing detection to identify infected hosts in large-scale enterprise networks. In 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) (pp. 479-490). IEEE.

Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. Arabian Journal for Science and Engineering, 45, 3171-3189.

Indre, I., & Lemnaru, C. (2016, September). Detection and prevention system against cyber attacks and botnet malware for information systems and Internet of Things. In 2016 IEEE 12th International Conference on Intelligent Computer Communication and Processing (ICCP) (pp. 175-182). IEEE.

Jing, T., Li, J., & Xing, R. (2012, February). Research on malicious links detection system based on script text analysis. In 2012 14th International Conference on Advanced Communication Technology (ICACT) (pp. 439-442). IEEE.

Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). Guide to cyber threat information sharing. NIST special publication, 800(150).

Kali Linux Tools. (n.d.). ettercap. Retrieved September 12, 2023, from https://www.kali.org/tools/ettercap/

Kali Linux Tools. (n.d.). hping3. Retrieved September 12, 2023, from https://www.kali.org/tools/hping3/

Kali Linux Tools. (n.d.). macchanger. Retrieved September 12, 2023, from https://www.kali.org/tools/macchanger/

Kurose, J. F., & Ross, K. W. (2017). *Computer networking: A top-down approach* (7th ed.). Pearson.

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review, 34(2), 39-53.

Nmap. (n.d.). Nmap Security Scanner. Retrieved September 12, 2023, from https://nmap.org/

Pangestu, T., & Liza, R. (2022). Analisis Keamanan Jaringan pada Jaringan Wireless dari Serangan Man In The Middle Attack DNS Spoofing. *JiTEKH*, *10*(2), 60-67.

Putra, M.R., & Pembimbing Achmad Imam Kistijantoro, S. (2011). ANALISIS DAN PENCEGAHAN SERANGAN MAN IN THE MIDDLE (MiTM) PADA OTENTIFIKASI WEB PROXY JARINGAN KAMPUS ITB.

Rachman, R. (2021). Analisis Keamanan Jaringan Wireless LAN (WLAN) Dengan Metode Penetration Testing Pada PT. PLN (Persero) Sektor Pengendalian Pembangkitan Pekanbaru (Doctoral dissertation, Universitas Islam Riau).

Riadi, I., Umar, R., & Busthomi, I. (2020). Optimasi Keamanan Autentikasi dari Man in the Middle Attack (MiTM) Menggunakan Teknologi Blockchain. Journal of Information Engineering and Educational Technology.

Ron, M. (2018, April). Situational status of global cybersecurity and cyber defense according to global indicators. Adaptation of a model for ecuador. In Developments and Advances in Defense and Security: Proceedings of the Multidisciplinary International Conference of Research Applied to Defense and Security (MICRADS 2018) (Vol. 94, p. 12). Springer.

Salazar Soler, J. (2017). Wireless networks. Czech Technical University of Prague.

Saputra, A. S., & Irwan, D. (2020). Sistem Keamanan Pada Jaringan Wireless Menggunakan Protokol RADIUS. JUSS (Jurnal Sains dan Sistem Informasi), 3(2), 28-34.

Telkom University. (n.d.). Kali Linux: Pengertian, Sejarah, Kelebihan, Kekurangan & Jenisnya. Retrieved September 12, 2023, from https://it.telkomuniversity.ac.id/kali-linux-pengertian-sejarah-kelebihan-kekurangan-jenisnya/

Telkom University. (n.d.). Pengertian Sistem Operasi Windows: Sejarah, Fungsi, dan Fiturnya. Retrieved September 12, 2023, from https://it.telkomuniversity.ac.id/pengertian-sistem-operasi-windows/

Valeriano, B., & Maness, R. C. (2018). International relations theory and cyber security. The Oxford handbook of international political theory, 259.

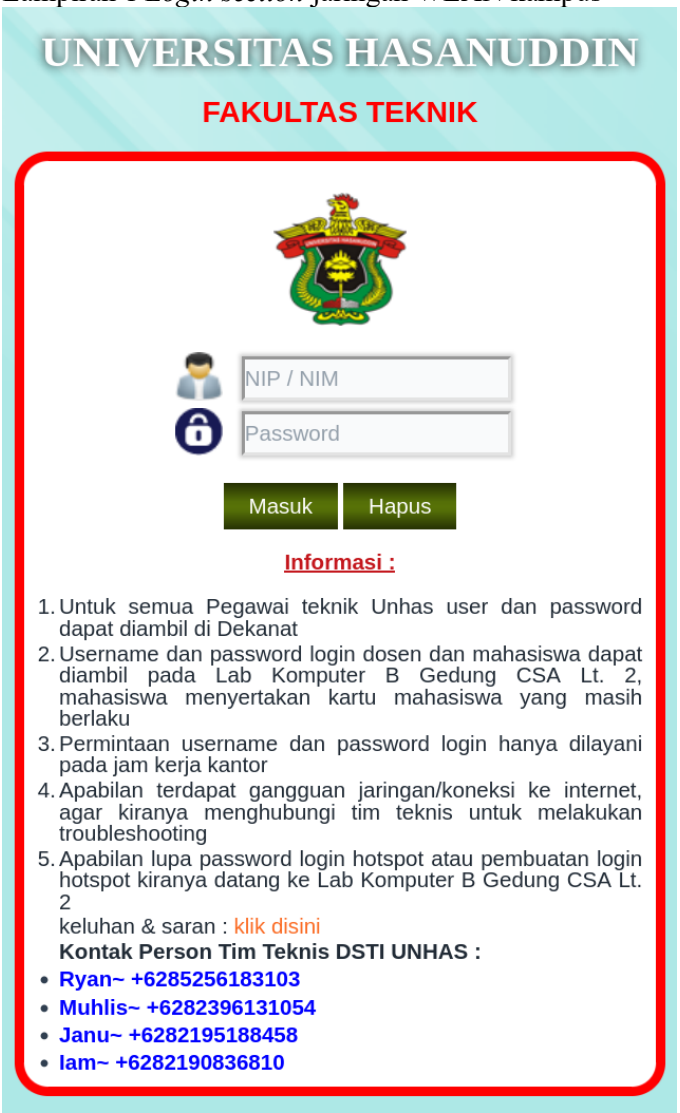
Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security–what goes where?. Information & Computer Security, 26(1), 2-9.

Wireshark. (n.d.). Frequently Asked Questions. Retrieved September 12, 2023, from https://www.wireshark.org/faq.html#_what_is_wireshark

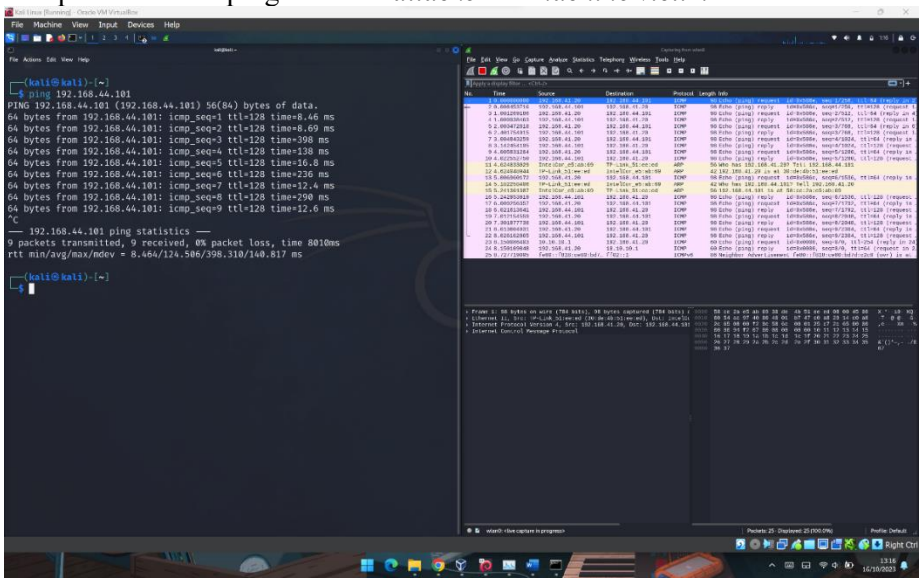
Zlomislić, V., Fertalj, K., & Sruk, V. (2017). Denial of service attacks, defences and research challenges. Cluster Computing, 20, 661-671.

LAMPIRAN

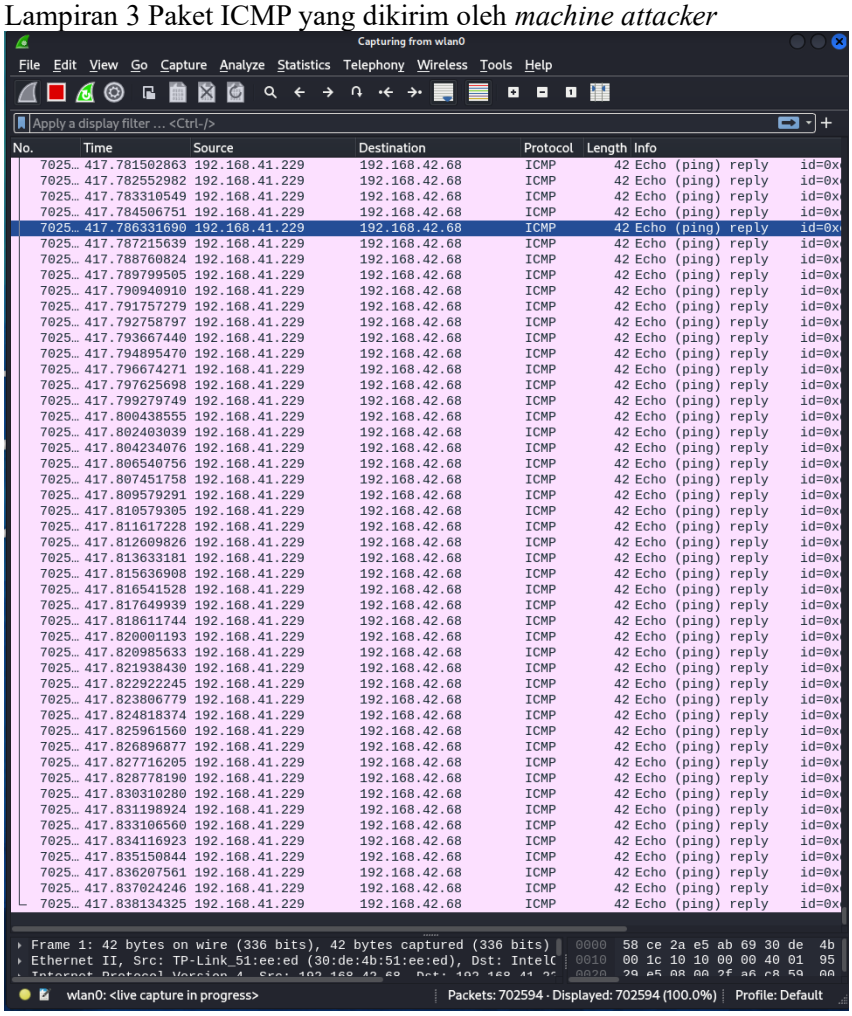
Lampiran 1 *Login section* jaringan WLAN kampus



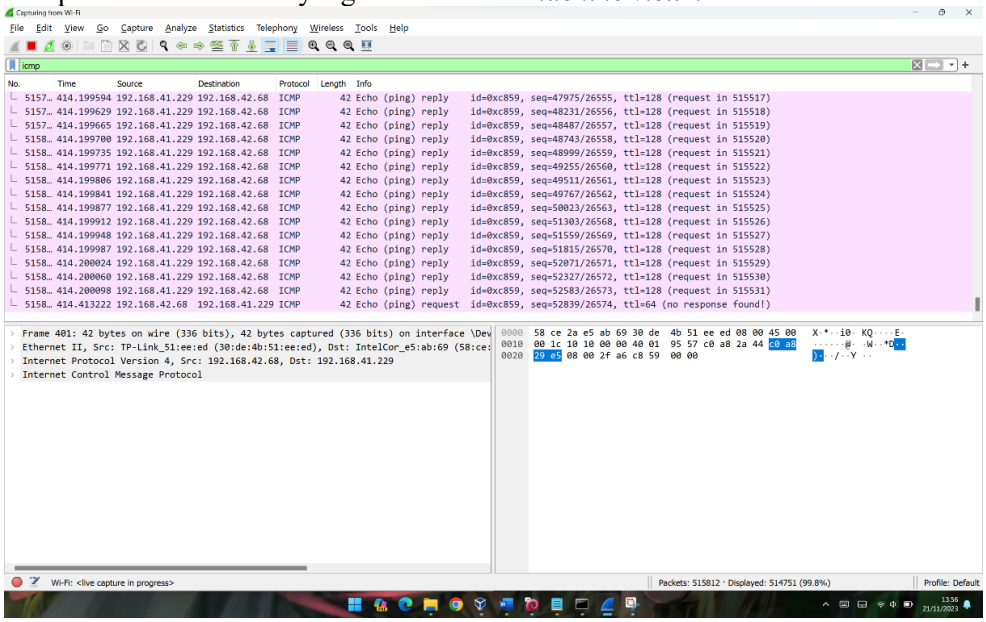
Lampiran 2 Trafik ping machine *attacker* ke *machine victim*



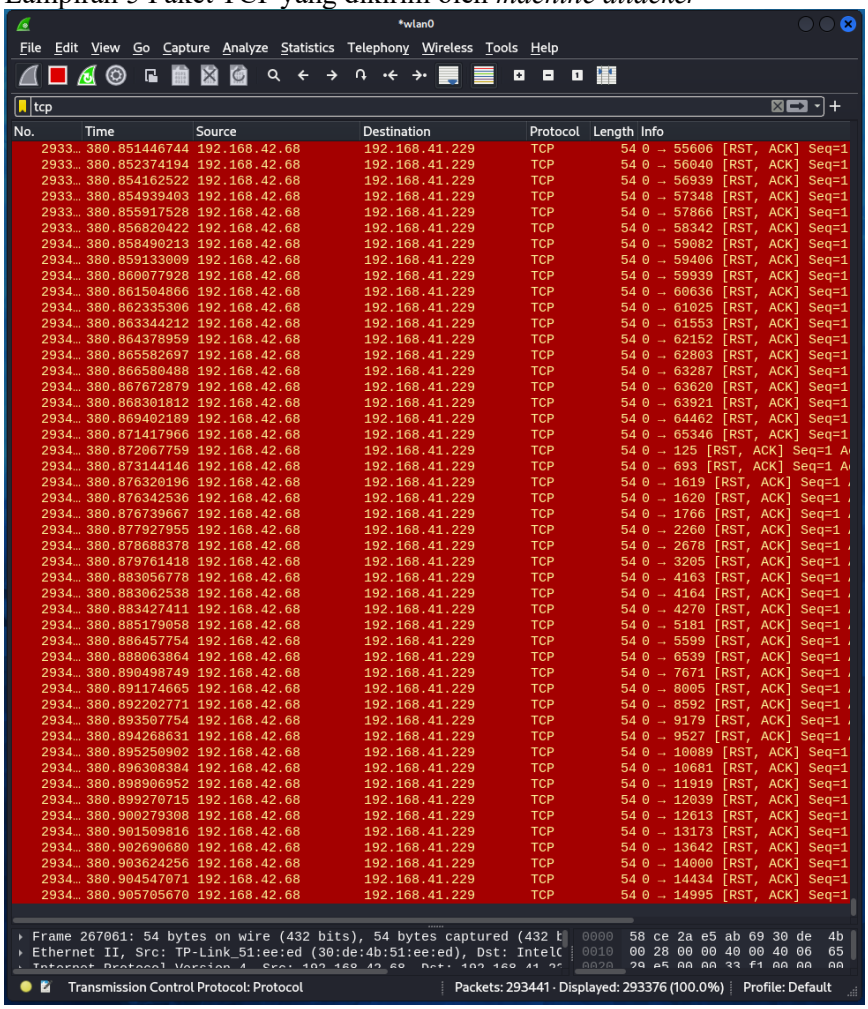
Lampiran 3 Paket ICMP yang dikirim oleh *machine attacker*



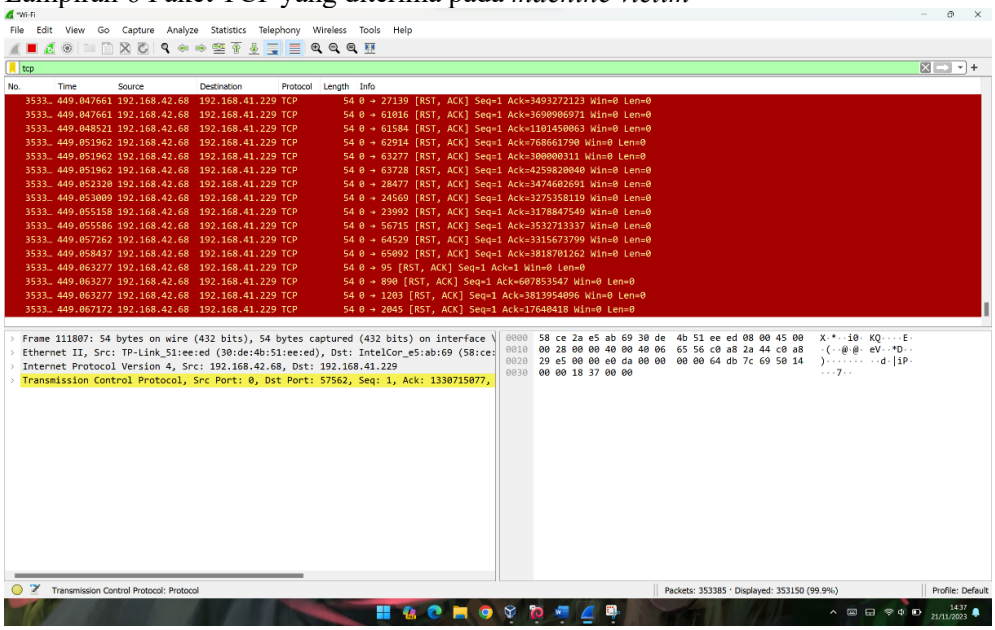
Lampiran 4 Paket ICMP yang diterima oleh *machine victim*



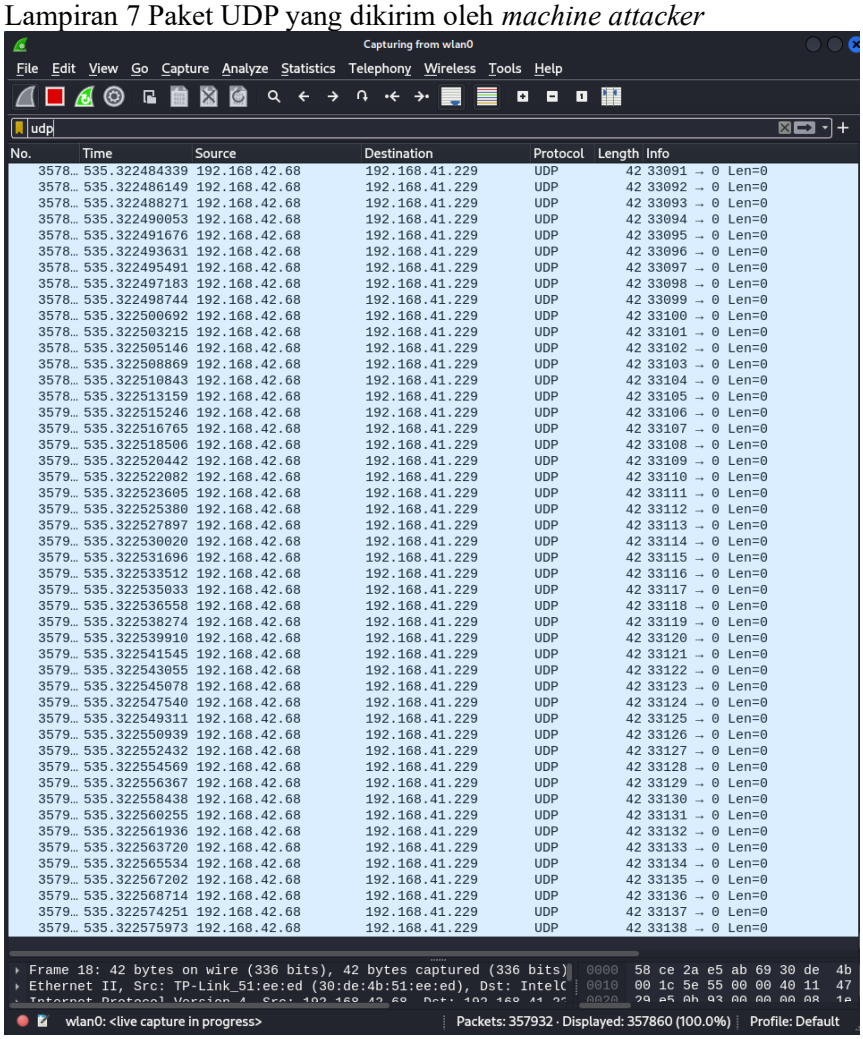
Lampiran 5 Paket TCP yang dikirim oleh *machine attacker*



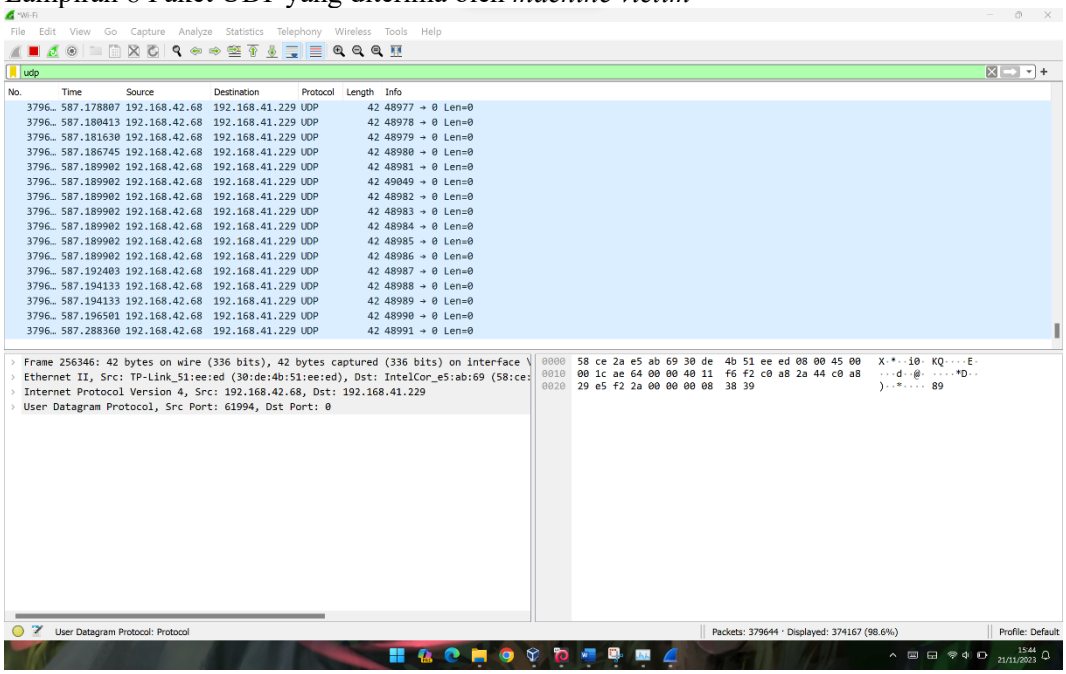
Lampiran 6 Paket TCP yang diterima pada *machine victim*



Lampiran 7 Paket UDP yang dikirim oleh *machine attacker*



Lampiran 8 Paket UDP yang diterima oleh *machine victim*



Lampiran 9 Trafik paket ARP yang diduplikasi dari *machine victim*