E-ISSN: 3031-8521
P-ISSN: 3032-1867

Halaman 3206-3218
Volume 3 Nomor 4 Tahun 2026

Reconstruction of Network Traffic Analysis of Suspected Emotet and IcedID Activity in a Public PCAP Dataset from a Privacy and Data Security Perspective

Alya Maura Raditha[1], Muhammad Rizky Bagas[2], Nabila Anggita Putri[3], Ade Kurniawan[4]

[1,2,3,4]Program Studi Sains Data, Institut Teknologi Sains Bandung, Kabupaten Bekasi, Indonesia
E-mail: alya.raditha@student.itsb.ac.id

Abstract

Downloader and banking malware such as Emotet and IcedID communicate over the network, so their traces can be observed in captured packets. The same traces also expose metadata that matters for privacy and data security. The study purpose was to reconstruct the network traffic analysis of a public packet capture (PCAP) dated 2018-12-18 (82,354 packets) and to interpret the findings from a privacy and data security perspective. Materials and methods. A descriptive-qualitative case study with offline network forensics in Wireshark was conducted, using conversation statistics, display filters, TCP stream following, and reading of User-Agent headers, MAC vendor prefixes, Kerberos, HTTP, and TLS Client Hello fields. Every statement was classified as a finding, an interpretation, or literature support. Results. The 172.16.3.0/24 segment contained Ubuntu, iPhone, Samsung tablet, Amazon, Android phone, and Windows devices. One host, 172.16.3.133, produced 18 HTTP and TLS packets within 844.03 seconds toward three IP addresses labelled Emotet and one labelled IcedID (SNI iamther.org). All labels and command-and-control status remain suspected, because payloads, file hashes, and intrusion-detection alerts were not available. Metadata such as IP addresses, computer names, User-Agent strings, and SNI revealed device identity and behaviour without exposing message content. Conclusions. The reconstruction is traceable to specific frames and yields indicators of compromise with explicit confidence levels. No evidence indicates that personal data were taken.

Keywords: *Network traffic analysis, Wireshark, Emotet, IcedID, Data privacy*

Abstrak

Malware pengunduh (*downloader*) dan perbankan (*banking malware*) seperti Emotet dan IcedID berkomunikasi melalui jaringan, sehingga jejak aktivitasnya dapat diamati melalui paket data yang berhasil ditangkap. Jejak yang sama juga dapat mengungkap metadata yang berkaitan dengan privasi dan keamanan data. Tujuan penelitian ini

adalah merekonstruksi analisis lalu lintas jaringan dari sebuah *public packet capture* (PCAP) tertanggal 18 Desember 2018 yang terdiri atas 82.354 paket, serta menginterpretasikan hasil temuannya dari perspektif privasi dan keamanan data. Bahan dan metode. Penelitian ini menggunakan pendekatan studi kasus deskriptif-kualitatif dengan teknik forensik jaringan secara luring menggunakan Wireshark. Analisis dilakukan melalui statistik komunikasi (*conversation statistics*), filter tampilan (*display filters*), penelusuran aliran TCP (*TCP stream following*), serta pembacaan *header User-Agent*, awalan vendor MAC, Kerberos, HTTP, dan kolom TLS Client Hello. Setiap pernyataan diklasifikasikan sebagai temuan, interpretasi, atau dukungan literatur. Hasil. Segmen jaringan 172.16.3.0/24 mencakup perangkat Ubuntu, iPhone, tablet Samsung, Amazon, ponsel Android, dan perangkat Windows. Salah satu host, yaitu 172.16.3.133, menghasilkan 18 paket HTTP dan TLS dalam rentang waktu 844,03 detik yang mengarah ke tiga alamat IP yang diberi label Emotet dan satu alamat IP yang diberi label IcedID (SNI iamther.org). Seluruh label tersebut dan statusnya sebagai server *command-and-control* masih bersifat dugaan karena data *payload*, *hash* file, dan peringatan dari sistem deteksi intrusi tidak tersedia. Metadata seperti alamat IP, nama komputer, rangkaian karakter User-Agent, dan SNI dapat mengungkap identitas serta perilaku perangkat tanpa harus memperlihatkan isi pesan yang dikomunikasikan.
Kesimpulan. Rekonstruksi analisis dapat ditelusuri berdasarkan nomor *frame* tertentu dan menghasilkan indikator kompromi (*indicators of compromise*) dengan tingkat keyakinan yang dinyatakan secara eksplisit. Tidak ditemukan bukti yang menunjukkan bahwa data pribadi telah diambil.

Kata kunci: *Analisis lalu lintas jaringan, Wireshark, Emotet, IcedID, privasi data.*

INTRODUCTION

Privacy is commonly understood as the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others (Westin, 2003). In data communication this claim depends on information security, that is, the protection of the confidentiality, integrity, and availability of information (National Institute of Standards and Technology Computer Security Resource Center [NIST CSRC], n.d.-a). In Indonesia, the duty to secure personal data and to notify failures of its protection is regulated by Law Number 27 of 2022 on Personal Data Protection (Republik Indonesia, 2022). The privacy risk management framework of the National Institute of Standards and Technology (Brooks et al., 2017) offers a way of thinking about risks to individuals and is referred to here only as a general framework.

One threat to all three aspects is malware, defined as software or firmware intended to perform an unauthorised process that harms the confidentiality, integrity, or availability of an information system (NIST CSRC, n.d.-b). Emotet and IcedID are two relevant examples. Boyarchuk et al. (2023) report that Emotet has data-theft modules, encrypted command-and-control (C2) communication, and access that is sold to other actors, while Çelik and Gezer (2022) classify it as a banking trojan that steals banking and personal data. MITRE (n.d.) describes IcedID as modular banking malware

observed since at least 2017 that uses HTTPS for C2 and can be downloaded by Emotet, and Center for Internet Security (2019) also notes that IcedID commonly arrives as a second-stage payload of other malware. A SANS Internet Storm Center diary reports an Emotet infection followed by IcedID, with TLS traffic to IcedID domains and GET /data2.php? requests carrying a hexadecimal parameter (Duncan, 2018).

Because malware must communicate to receive instructions or send data, it leaves traces in network traffic. Packet analysis is positioned as a technique for tracing and proving events in network forensics (Sikos, 2020), with open challenges mapped by Khan et al. (2016). Wireshark has been used to identify C2, HTTP, and DNS communication that was then confirmed with a scanning service (Tampubolon et al., 2024). However, HTTP-based C2 resembles ordinary web traffic (Acarali et al., 2016), and the content of TLS sessions cannot be inspected without additional inspection models (Oh, Ha, & Roh, 2022). Analysts therefore often hold only metadata and must distinguish what is directly visible from what is only suspected.

Metadata is itself valuable to an observer. Shamsimukhametov et al. (2022) show that Encrypted ClientHello, which hides the SNI from network observers, degrades the performance of existing traffic classifiers, so the SNI can be regarded as informative metadata. Hu and Fukuda (2023) show that the categories of websites visited by users can still be inferred from encrypted DNS traffic, whatever the protocol. Both findings confirm that a privacy discussion of traffic analysis does not stop at message content.

Among the sources reviewed in this study, attention has centred on tracking Emotet infrastructure (Boyarchuk et al., 2023), automated detection (Çelik & Gezer, 2022), and surveys of packet and encrypted-traffic analysis techniques (Khan et al., 2016; Oh et al., 2022; Sikos, 2020). No documentation was found of a manual replication on a public practice dataset that explicitly separates direct evidence, interpretation, and literature support and then interprets the result from a privacy perspective. This statement is limited to the sources reviewed and is not a claim that the topic has never been addressed elsewhere.

The study purpose was (1) to reconstruct the analysis process on the 2018-12-18 PCAP to identify devices in the network; (2) to characterise the communication of a suspected infected host with external infrastructure; (3) to formulate indicators of compromise (IoC) with their confidence levels; and (4) to interpret the findings from a privacy and data security perspective. Documentation that separates findings, interpretations, and suspicions helps learners and practitioners replicate similar analyses with a clear evidence trail. The contribution is methodological and documentary, not a new detection method.

METHOD

Research design and workflow

This study is a descriptive-qualitative case study using network forensics on a single PCAP file analysed offline. The approach was chosen because the aim is to trace and explain, not to measure the performance of an algorithm. The workflow has seven

stages, shown in Figure 1: loading the PCAP file, reading conversation statistics, identifying devices, filtering the prominent host, building a timeline, formulating IoC with confidence levels, and interpreting the findings from a privacy and data security perspective. All result claims come from the author's practice documentation in the form of Wireshark screenshots, while the exercise page and its answer document were used only as a comparison to check consistency.

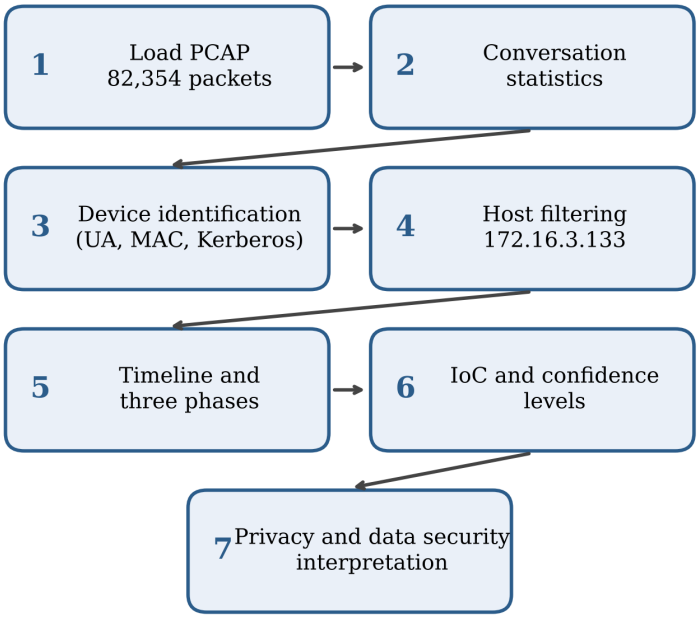


Figure 1. Research workflow

In the first stage the PCAP file was loaded into Wireshark offline. The packet count, 82,354, was recorded as the basis for all later calculations, and no packet was sent back to any network. The second stage read the conversation statistics through Statistics > Conversations, which gives the number of IPv4 and UDP conversations, the LAN segment range, and the sources of DHCP and Kerberos packets that indicate server roles.

The third stage identified devices. The display filters in Table 1 were used to find User-Agent headers, session content was read with Follow > TCP Stream, vendors were read from MAC address prefixes, and computer names were read from the CNameString field of Kerberos packets. The fourth stage filtered the prominent host, 172.16.3.133: its HTTP and TLS Client Hello packets were displayed without SSDP traffic (UDP 1900), and the destination, URL path, and SNI value were noted for each packet.

The fifth stage built the timeline. Packets were ordered by Wireshark relative time, the interval between two packets was calculated as $\Delta t = tb - ta$, the span of a host's activity as $T = tn - t1$, and activity was grouped into phases by prominent time gaps. The sixth stage formulated IoC: destination IP addresses, SNI, and URL paths of the prominent host were recorded with frame numbers, labelled as suspected according to

network patterns, and assigned confidence levels. The seventh stage interpreted the findings in terms of privacy and information security (NIST CSRC, n.d.-a; Westin, 2003), and of the obligations in Indonesian regulation (Republik Indonesia, 2022), without concluding that a violation occurred.

Data and environment

The data are the file 2018-12-18-traffic-analysis-exercise.pcap from the Malware-Traffic-Analysis.net traffic analysis exercise (Malware-Traffic-Analysis.net, 2018), which contains 82,354 packets. The exercise scenario describes the LAN 172.16.3.0/24. The exercise page gives no author name, so the source is recorded as the site itself. The Wireshark version and the start and end times of the capture [PERLU KONFIRMASI]. The analysis was fully offline: the malware was not executed, and no IP address or domain was contacted. User account names are not reproduced in this article.

Analysis procedure and display filters

Table 1 lists the display filters used. The Ubuntu filter is written without quotation marks, while the value “8.0.0” uses quotation marks because it is a dotted numeric string.

Table 1. Display filters used

Filter	Function
ip contains Ubuntu and http.request	Finds User-Agent containing Ubuntu
ip.addr eq 172.16.3.188 and http.request	HTTP requests from 172.16.3.188
ip.addr eq 172.16.3.112 and http.request	HTTP requests from 172.16.3.112
ip contains "8.0.0" and http.request	Finds User-Agent of Android 8.0.0
kerberos.CNameString	Shows computer or account name in Kerberos packets
(http.request or ssl.handshake.type == 1) and !(udp.port eq 1900) and ip.addr eq 172.16.3.133	HTTP and TLS Client Hello of host 172.16.3.133 without SSDP (UDP 1900) traffic

Evidence levels and labelling

Every statement is separated into a finding (directly visible in packets), an interpretation (reasoning from findings), and literature support. The labels “Emotet” and “IcedID” in the packet list are the author's annotations based on network patterns, marked with † and kept as suspected, because there is no file hash, scanning-service report, or intrusion-detection alert.

RESULT AND DISCUSSION

Network environment and device identification

Figure 2 shows the result of Statistics > Conversations with 599 IPv4 conversations and 851 UDP conversations from 82,354 packets. The LAN segment is 172.16.3.0/24. The DHCP Offer and Kerberos TGS-REP packets originate from

172.16.3.2, and clients use 8.8.8.8 as the DNS server. The role of 172.16.3.2 as a domain controller and of Cisco_a2:bf:89 as a gateway are the author's interpretations.

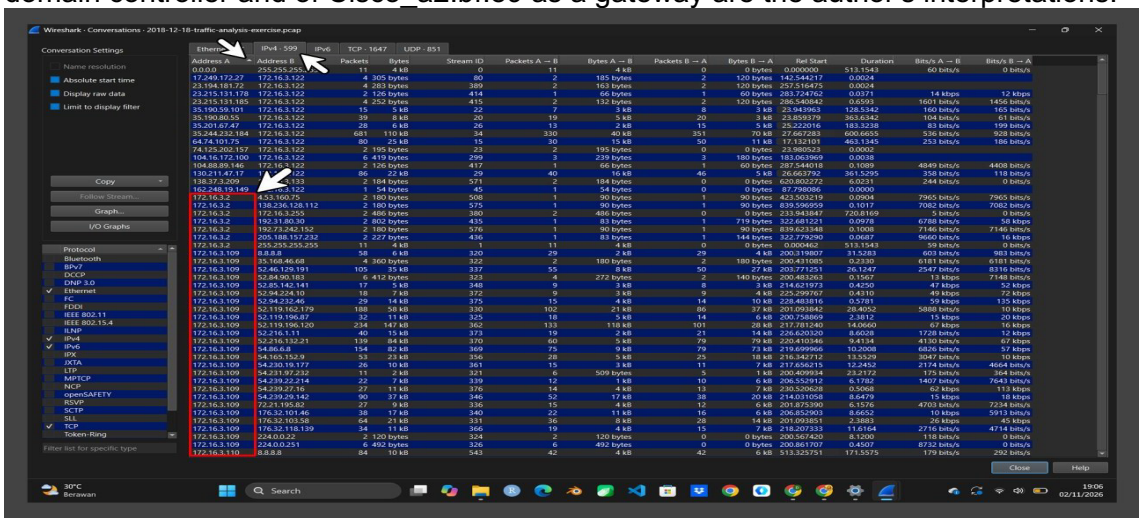


Figure 2. IPv4 conversation statistics in the PCAP (Statistics > Conversations)

Figure 3 shows the Kerberos TGS-REP packet (frame 35206) with realm EGGNOGSOUP.COM and CNameString GOODSON-WIN-PC$. The "$" sign indicates a computer account, not a user account.

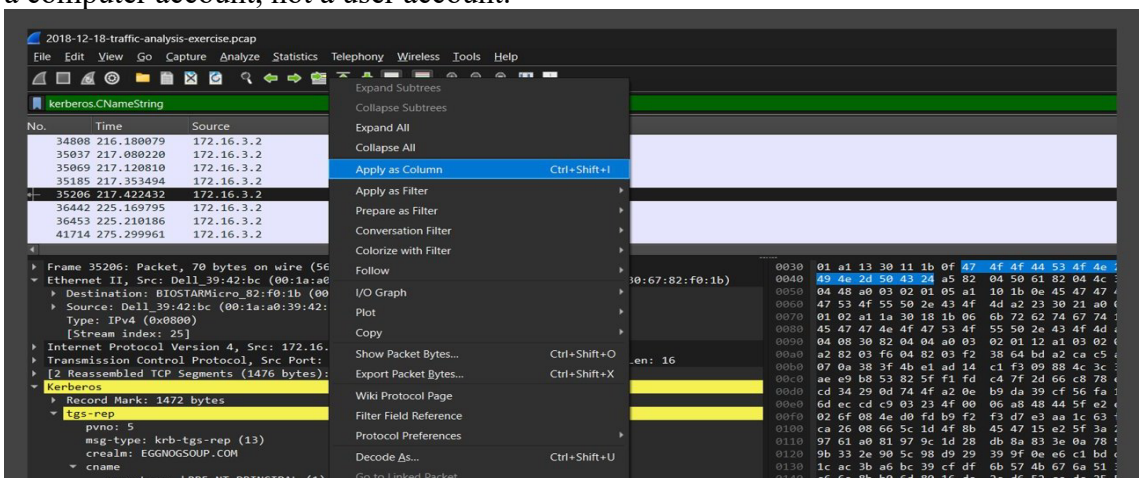


Figure 3. Detail of the Kerberos TGS-REP packet showing CNameString GOODSON-WIN-PC$

The identified devices are summarised in Table 2. The identification of 172.16.3.110, 172.16.3.188, and 172.16.3.112 is directly supported by the HTTP User-Agent headers in Figure 4. Device 172.16.3.109 is recognised only from its MAC vendor, so its type is not concluded. For 172.16.3.112, the model code SM-T113 matches more than one Samsung product name, so the model is written only as that code.

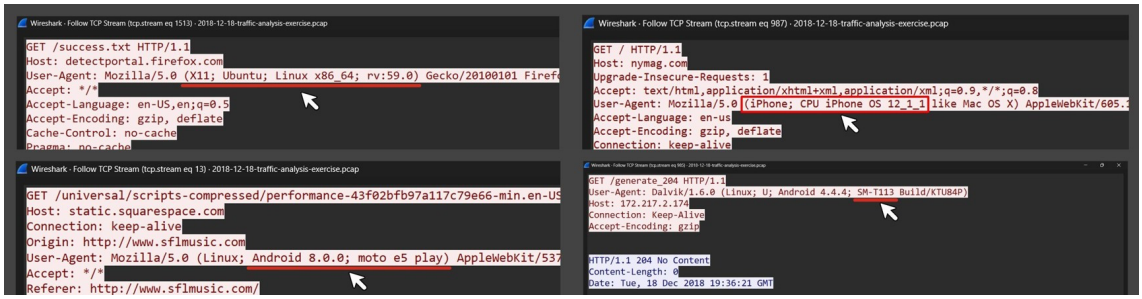


Figure 4. User-Agent evidence in Follow TCP Stream: Ubuntu Linux (top left), iPhone iOS 12.1.1 (top right), Android 8.0.0 moto e5 play (bottom left), and Android 4.4.4 SM-T113 (bottom right)

Table 2. Devices identified on the 172.16.3.0/24 network

IP	Device / OS	MAC (vendor)	Evidence
172.16.3.110	Ubuntu Linux x86_64, Firefox rv:59.0	Intel_d9:44:b9	HTTP User-Agent
172.16.3.188	iPhone, iOS 12.1.1	Apple_c1:99:a5	HTTP User-Agent
172.16.3.112	Samsung SM-T113, Android 4.4.4	SamsungElect_99:41:07	HTTP User-Agent
172.16.3.109	Type not concluded	AmazonTechno_d2:5e:47	MAC vendor
Not shown	Android 8.0.0, moto e5 play	Not available	HTTP User-Agent
Not shown	Windows, GOODSON-WIN-PC$	Not available	Kerberos (frame 35206)
172.16.3.133	Presumably Windows	ASUSTekCOMPU_bf:04:13	MAC vendor; /ncsi.txt (frame 12461)

Activity of host 172.16.3.133

The last filter in Table 1 displays 18 HTTP and TLS Client Hello packets for host 172.16.3.133 (Figure 5). Their relative times range from 130.154939 s to 974.186266 s, so T = 844.031327 s. A summary of the packets grouped by destination is given in Table 3.

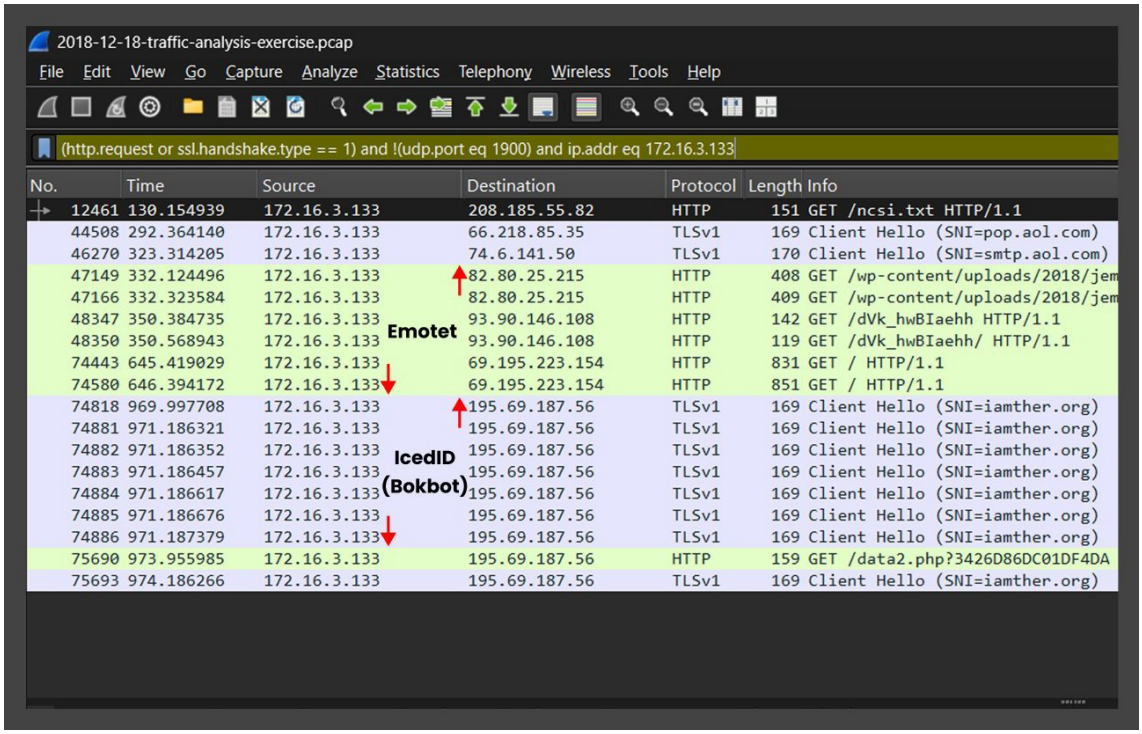


Figure 5. The 18 HTTP and TLS Client Hello packets of host 172.16.3.133 with the author's annotations (Emotet† and IcedID†)

Table 3. Summary of the 18 packets of host 172.16.3.133 by destination

Frame	Time (s)	Destination IP	Protocol; content	Label†
12461	130.154939	208.185.55.82	HTTP; GET /ncsi.txt	Context
44508, 46270	292.364140; 323.314205	66.218.85.35; 74.6.141.50	TLS Client Hello; SNI pop.aol.com and smtp.aol.com	Context
47149, 47166	332.124496; 332.323584	82.80.25.215	HTTP; GET /wp-content/uploads/2018/… and …/Companies-Invoice-0970945/ (URL truncated)	Emotet†
48347, 48350	350.384735; 350.568943	93.90.146.108	HTTP; GET /dVk_hwBIaehh and /dVk_hwBIaehh/	Emotet†
74443, 74580	645.419029; 646.394172	69.195.223.154	HTTP; GET / (831 and 851 bytes)	Emotet†
74818, 74881–74886, 75693	969.997708–974.186266	195.69.187.56	TLS Client Hello (8 packets); SNI iamther.org	IcedID†

Frame	Time (s)	Destination IP	Protocol; content	Label†
75690	973.955985	195.69.187.56	HTTP; GET /data2.php?3426D86DC01DF4DA	IcedID†

†Author's annotation, not an automated detection result. Ports are not visible in the screenshot.

The activity falls into three phases (Figure 6). The first phase (130.15–323.31 s) consists of a Windows connectivity check and TLS sessions to AOL mail servers, which are not used as IoC. The second phase (332.12–646.39 s) contains HTTP requests to three different IP addresses; the interval from the first request to 82.80.25.215 (frame 47149) to the last request to 69.195.223.154 (frame 74580) is 314.27 s. The third phase (969.998–974.186 s) contains TLS connections and one HTTP request to 195.69.187.56, 323.60 s after the second phase.

In the second phase, two IP addresses received pairs of requests very close together (0.199 s and 0.184 s), and the requests to 69.195.223.154 are 0.975 s apart with frame lengths of 831 and 851 bytes, much larger than other requests in the same phase (119–409 bytes). Six of the eight Client Hello packets to iamther.org (frames 74881–74886) occur within 0.001058 s.

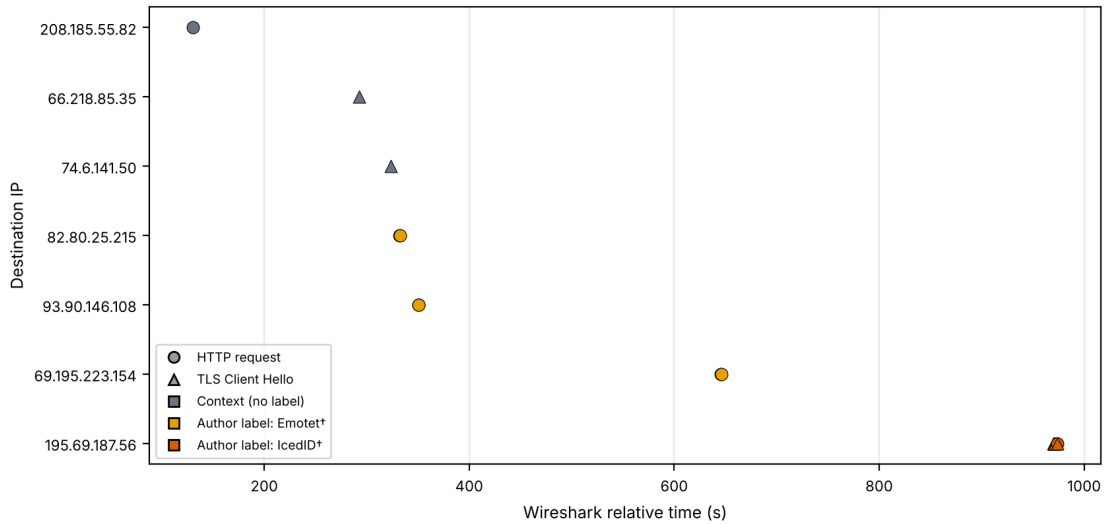


Figure 6. Time sequence of the 18 packets of host 172.16.3.133 (prepared by the authors from the data in Figure 5)

Indicators of compromise and confidence levels

All IoC in Table 4 come from the PCAP. Addresses in the first phase are recorded as context and are not IoC. File-based indicators can be formulated once file names and hashes are obtained from Export Objects.

Table 4. Indicators of compromise and their confidence levels

Type	Value	Frame	Status and confidence
IP	82.80.25.215	47149, 47166	Suspected (Emotet† label); low
IP	93.90.146.108	48347, 48350	Suspected (Emotet† label); low
IP	69.195.223.154	74443, 74580	Suspected (Emotet† label); low
IP	195.69.187.56	74818–75693	Suspected C2 (IcedID† label); low
Domain (SNI)	iamther.org	74818, 74881–74886, 75693	Suspected C2 (IcedID† label); low
URL path	/dVk_hwBIaehh; /data2.php?3426D86DC01DF4DA	48347, 48350; 75690	Suspected; low
Observation	172.16.3.133 contacted four external IPs with unusual patterns	Table 3	High, as an observed fact

†Author's annotation.

Interpretation of communication patterns

The patterns of the second and third phases agree with the picture that Emotet acts as a downloader of other malware and that IcedID can be downloaded by Emotet (Center for Internet Security, 2019; MITRE, n.d.). The SANS ISC diary also contains *GET /data2.php?* requests with a hexadecimal parameter and TLS connections to an IcedID domain in an Emotet infection (Duncan, 2018), similar in form to frame 75690 and the Client Hello packets to iamther.org. This similarity strengthens the suspicion but does not prove it. Because the server responses, content types, and downloaded files are not part of the documentation, the hypothesis that the repeated requests are retries or redirect following is recorded as a direction for further testing. Similar conditions are described in the literature: HTTP-based C2 resembles ordinary web traffic (Acarali et al., 2016), and TLS content cannot be read, so the SNI gives only indirect indications (Oh et al., 2022). The Emotet† and IcedID† labels therefore remain suspected.

Privacy and data security implications

Although message content cannot be read, the metadata in the PCAP already contains privacy-related information. Kerberos packets reveal the realm and computer name, the User-Agent reveals the operating system and device model, the MAC prefix reveals the vendor, and the SNI and unencrypted HTTP requests reveal connection destinations and URL paths. From this combination an analyst can map the devices and connection behaviour of every host without opening any message. This agrees with the literature that the SNI is informative metadata to an observer (Shamsimukhametov et al., 2022) and that encrypted traffic can still leak information about user activity (Hu & Fukuda, 2023). Protecting content (encryption) therefore does not automatically protect metadata, and the storage and sharing of PCAP files should be treated as handling potentially sensitive data.

This study found no evidence that personal data were taken. The practice contains only 18 HTTP and TLS packets without content, hashes, or alerts, so no statement about data

theft or failure of personal data protection can be made. The assessment that can be given is conditional: if a host like this were in a real environment, an indication of communication with suspected malicious infrastructure would be a reason to examine the host further, including whether it holds personal data that must be protected under the obligations in Republik Indonesia (2022). This assessment is not a legal conclusion.

Consistency with the comparison document

Compared with the exercise answer document, the author's practice is consistent on the Ubuntu host (172.16.3.110), the iPhone (172.16.3.188), the host indicating infection (172.16.3.133), the brand and model of the Android 8.0.0 phone, and device 172.16.3.112. The answer document also lists host names, domain names, and ports that do not appear in the author's screenshots; this information is not included as a result because it does not come from this practice. The count of all active hosts and the full list of device IP addresses are outside the scope of this practice and are not claimed as results.

CONCLUSIONS

The reconstructed analysis of the 2018-12-18 PCAP identified the main devices on the 172.16.3.0/24 network and located 172.16.3.133 as a suspected infected host, with 18 HTTP and TLS packets divided into three phases over 844.03 s. Communication with three IP addresses labelled Emotet† and with 195.69.187.56 (iamther.org) labelled IcedID† yields IoC consisting of four IP addresses, one SNI domain, and URL paths, all with suspected status because there is no payload, hash, or detection alert. From a privacy perspective, metadata alone is enough to reveal device identity and behaviour, but there is no evidence that personal data were obtained.

The strengths of this approach are that every claim can be traced to a frame, a time, and a filter, and that findings, interpretations, and suspicions are consistently separated. Its weaknesses are the dependence on screenshot documentation without payloads or detection alerts, and the absence of a quantitative evaluation on a single practice PCAP that does not represent the variety of infrastructure of the two malware families. Further research can complete the counts of hosts and IP addresses for all devices, Export Objects with SHA256 hashes and scanning-service checks, HTTP stream content, the TLS certificate of 195.69.187.56, DNS queries, and intrusion-detection alerts, so that the classification and C2 status can be tested more strongly.

Acknowledgement

The authors thank Malware-Traffic-Analysis.net for providing a practice dataset that is open to the public. Thanks to supervisors or other supporting partiess.

REFERENCES

Acarali, D., Rajarajan, M., Komninos, N., et al. (2016). Survey of approaches and features for the identification of HTTP-based botnet traffic. Journal of Network and Computer Applications, 76, 1–15. https://doi.org/10.1016/j.jnca.2016.10.007

Boyarchuk, O., Mariani, S., Ortolani, S., et al. (2023). Keeping up with the Emotets: Tracking a multi-infrastructure botnet. Digital Threats: Research and Practice, 4(3), Article 41. https://doi.org/10.1145/3594554

Brooks, S., Garcia, M., Lefkovitz, N., et al. (2017). An introduction to privacy engineering and risk management in federal systems (NIST IR 8062). National Institute of Standards and Technology. Retrieved from https://csrc.nist.gov/pubs/ir/8062/final

Çelik, R., & Gezer, A. (2022). Detection of Trickbot and Emotet banking trojans with machine learning. Balkan Journal of Electrical and Computer Engineering, 10(4), 377–387. https://doi.org/10.17694/bajece.1031021

Center for Internet Security. (2019, September 18). Security primer: IcedID. Retrieved from https://www.cisecurity.org/insights/white-papers/security-primer-icedid

Duncan, B. (2018, November 15). Emotet infection with IcedID banking Trojan (Diary 24312). SANS Internet Storm Center. Retrieved from https://isc.sans.edu/diary/24312

Hu, G., & Fukuda, K. (2023). Characterizing privacy leakage in encrypted DNS traffic. IEICE Transactions on Communications, E106.B(2), 156–165. https://doi.org/10.1587/transcom.2022EBP3014

Khan, S., Gani, A., Wahab, A. W. A., et al. (2016). Network forensics: Review, taxonomy, and open challenges. Journal of Network and Computer Applications, 66, 214–235. https://doi.org/10.1016/j.jnca.2016.03.005

Malware-Traffic-Analysis.net. (2018). 2018-12-18 – Traffic analysis exercise – Eggnog soup. Retrieved from https://www.malware-traffic-analysis.net/2018/12/18/index.html

MITRE. (n.d.). IcedID, software S0483. MITRE ATT&CK. Retrieved from https://attack.mitre.org/software/S0483/

National Institute of Standards and Technology Computer Security Resource Center. (n.d.-a). Information security. In Glossary. Retrieved from https://csrc.nist.gov/glossary/term/information_security

National Institute of Standards and Technology Computer Security Resource Center. (n.d.-b). Malware. In Glossary. Retrieved from https://csrc.nist.gov/glossary/term/malware

Oh, C., Ha, J., & Roh, H. (2022). A survey on TLS-encrypted malware network traffic analysis applicable to security operations centers. Applied Sciences, 12(1), 155. https://doi.org/10.3390/app12010155

Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196. Retrieved from https://peraturan.bpk.go.id/details/229798/uu-no-27-tahun-2022

Shamsimukhametov, D., Kurapov, A., Liubogoshchev, M., et al. (2022). Is encrypted ClientHello a challenge for traffic classification? IEEE Access, 10, 77883–77897. https://doi.org/10.1109/ACCESS.2022.3191431

Sikos, L. F. (2020). Packet analysis for network forensics: A comprehensive survey. Forensic Science International: Digital Investigation, 32, 200892. https://doi.org/10.1016/j.fsidi.2019.200892

Tampubolon, P., Putri, E. L., Zalianti, N. R., et al. (2024). Identifikasi malware pada Wireshark. Jurnal Kajian Teknik Elektro, 9(1), 64–68. https://doi.org/10.52447/jkte.v9i1.8004

Westin, A. F. (2003). Social and political dimensions of privacy. Journal of Social Issues, 59(2), 431–453. https://doi.org/10.1111/1540-4560.00072