

**SOSIALISASI PENGENALAN PERANGKAT LUNAK BERBAHAYA (MALWARE) DI SD
NEGERI 45/IV KOTA JAMBI**

Diah Aprilita Nizar¹, Rizal Kulfikri², Noprizal Faziri³

¹²³Prodi Sistem Informasi, Fakultas sains dan teknologi,
Universitas Sulthan Thaha Saifudin Jambi

Email: ¹diahapni28@gmail.com, rizalkulfikri899@gmail.com,
³rizaltehgelas9@gmail.com

Abstract

In today's rapidly developing digital era, data and computer system security is an important thing to maintain, especially against malicious software (malware) attacks, which can attack and threaten the security of data and computer systems, these threats can be in the form of viruses, ransomware, trojans, worms, and spyware. This socialization activity aims to provide an understanding to elementary school students about malicious software (malware) that can threaten the security of data and computer systems. Through this activity, it is hoped that students will be able to recognize the forms of malware and understand the steps to prevent them early. The implementation method is carried out through presentations using power point media with an interactive approach so that students can more easily understand the material presented. The socialization was held on Tuesday, September 16, 2025, at 08.00 at SDN 45 / IV Jambi City with participants from grades 5 and 6. The results of the activity showed high enthusiasm from the participants and an increase in basic understanding of the dangers of malware and how to prevent them, with this activity, students are expected to be wiser and more careful in using digital devices.

Keywords: Malware, Internet, Socialization, Digital Security, SD 45/IV Kota Jambi

Abstrak

Dalam era digital yang berkembang pesat seperti sekarang ini, keamanan data dan sistem computer menjadi hal yang penting untuk dijaga, terutama terhadap serangan perangkat lunak berbahaya (malware), yang dapat menyerang dan mengancam keamanan data maupun sistem computer, ancaman tersebut bisa saja berupa virus, ransomware, trojan, worm, dan spyware. Kegiatan sosialisasi ini bertujuan untuk memberikan pemahaman kepada siswa sekolah dasar mengenai perangkat lunak berbahaya (malware) yang dapat mengancam keamanan data dan sistem computer. Melalui kegiatan ini, diharapkan siswa mampu mengenali bentuk-bentuk malware dan memahami langkah pencegahannya sejak dini. Metode pelaksanaan dilakukan melalui presentasi menggunakan media power point dengan pendekatan interaktif agar siswa lebih mudah memahami materi yang disampaikan. Sosialisasi dilaksanakan pada hari Selasa, 16 September 2025, pukul 08.00 di SDN 45/IV Kota Jambi dengan peserta siswa kelas 5 dan 6. Hasil kegiatan menunjukkan antusiasme tinggi dari peserta dan peningkatan pemahaman dasar mengenai bahaya malware serta cara mencegahnya, dengan adanya kegiatan ini, siswa diharapkan lebih bijak dan berhati-hati dalam menggunakan perangkat digital.

Kata kunci: Malware, Internet, Sosialisasi, Keamanan Digital, SDN 45/IV Kota Jambi

Article History

Received: November 2025

Reviewed: November 2025

Published: November 2025

Plagiarism Checker No 619

Prefix DOI: Prefix DOI:

10.8734/sindoro.v1i2.360

Copyright: Author

Publish by: SINDORO



This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).

1. Latar Belakang

Di era digital yang berkembang pesat ini, anak-anak Indonesia khususnya siswa kelas tinggi sekolah dasar (SD) berusia 12-13 tahun, semakin akrab dengan teknologi. Data dari UNICEF (2022) menunjukkan bahwa 71% populasi global usia 15-24 tahun telah terkoneksi internet, sebuah tren yang juga signifikan pada kelompok usia yang lebih muda. Di Indonesia sendiri, survei APJII (2024), melaporkan bahwa 34,40% pengguna internet berusia 12-27 tahun. Fenomena ini menjadikan literasi digital dan keamanan online sebagai keterampilan esensial abad ke-21, sebuah pilar pendidikan modern yang sejajar dengan kemampuan membaca, menulis dan berhitung, seperti yang diakui oleh UNESCO (2021). Namun tingginya ketergantungan terhadap teknologi juga diikuti meningkatnya potensi ancaman keamanan digital terutama dari perangkat lunak berbahaya atau *malware* (Satria, W., Prayoga, J., & Does, E., 2025).

Malware merupakan istilah yang berasal dari gabungan kata “*Malicious*” dan “*Software*”, yang berarti perangkat lunak berbahaya. *Malware* dirancang untuk menyusup, merusak, atau mengeksploitasi sistem komputer tanpa seizin pengguna. Secara umum, *malware* mencakup berbagai bentuk ancaman siber, seperti virus, worm, ransomware, spyware, dan lainnya (Stalling & Brown, 2020). *Malware* dapat menyebar dengan cepat di jaringan tanpa campur tangan dari pengguna. Sistem pendeteksian *malware* masih menjadi masalah karena varian *malware* baru yang selalu berkembang dengan menggunakan teknik yang berbeda untuk menghindari metode pendeteksian. Sasaran utama dari *malware* adalah untuk memata-matai seseorang, mencuri informasi atau data pribadi, dan lain-lainnya.

Di Indonesia, ancaman siber terus meningkat dari tahun ke tahun, berdasarkan analisis Napila et al., (2025), pendidikan menjadi sektor utama serangan siber karena lemahnya sistem keamanan jaringan dan rendahnya kesadaran pengguna terhadap perlindungan data, serta rendahnya kesadaran keamanan di kalangan siswa SD di Indonesia. Studi Kaspersky (2024) melaporkan bahwa 68% anak usia 10-12 tahun tidak sengaja terpapar konten tidak pantas. Ancaman digital kini semakin kompleks, mulai dari phishing, oversharing data pribadi, hingga perundungan siber yang terus berevolusi. Sayangnya, pemahaman siswa SD mengenai jejak digital dan privasi masih tergolong rendah (Karim, W. N., & Kurniawan, A. J., 2025).

Serangan *malware* umumnya menargetkan institusi yang memiliki sistem keamanan lemah serta sumber daya yang terbatas dalam menangani ancaman siber. Oleh karena itu, sekolah tidak hanya perlu memperkuat infrastruktur keamanannya, tetapi juga memberikan edukasi yang memadai kepada seluruh pemangku kepentingan. Upaya pencegahan tidak hanya bergantung pada peningkatan teknologi keamanan, tetapi juga pada peningkatan kesadaran dan literasi keamanan siber bagi seluruh komunitas pendidikan. Schneier (2019) menegaskan bahwa kesadaran pengguna merupakan lapisan pertahanan terpenting dalam keamanan siber. Dengan demikian, kegiatan pengabdian masyarakat ini bertujuan untuk memperkenalkan konsep *malware* serta langkah-langkah pencegahannya guna meningkatkan perlindungan data siswa.

SDN 45/IV Kota Jambi merupakan salah satu lembaga pendidikan yang siswanya adalah anak-anak yang sudah memulai menggunakan internet. Sampai saat ini, belum pernah dilakukan sosialisasi khusus mengenai *malware*, padahal materi ini seperti ini penting agar siswa memahami konsep dan cara pencegahan infeksi *malware*. Oleh karena itu, melalui kegiatan pengabdian kepada masyarakat ini, kami akan menyelenggarakan sosialisasi terkait pengenalan, konsep, dan pengaduan pencegahan *malware* kepada siswa SDN 45/IV Kota Jambi. Kegiatan ini diharapkan dapat menjadi pembelajaran yang membantu siswa menghindari potensi infeksi maupun eksploitasi *malware* yang banyak tersebar di internet.

2. Metode Penelitian

Dalam kegiatan pengabdian kepada masyarakat terkait *malware* ini di laksanakan menggunakan metode sosialisasi edukasi partisipatif yang menekankan keterlibatan aktif peserta dalam proses pembelajaran. Pendekatan ini dipilih karena efektif untuk memperkenalkan konsep dasar keamanan digital melalui interaksi langsung antara pemateri dan peserta. Materi yang di sampaikan berupa pengenalan apa itu *malware*, jenis-jenis *malware* dan cara pencegahannya. Setelah kegiatan penyampaian materi selesai adapun kegiatan yang dilakukan selanjutnya yaitu dilanjutkan dengan sesi tanya jawab.

Berikut adalah beberapa tahapan yang dilakukan saat pelaksanaan pengabdian kepada masyarakat di SDN 45/IV Kota Jambi.

a. Tahap Persiapan

Pada tahap persiapan ini meliputi beberapa kegiatan yaitu :

1) Kunjungan awal

Pada tahap ini dilakukan kunjungan ke lokasi yang akan diselenggarakannya sosialisasi yakni di SDN 45/IV Kota Jambi yang berlokasi di Jl. Husni Thamrin, Beringin, Kec. Ps. Jambi, Kota Jambi. Kunjungan ini di lakukan untuk bertukar informasi antara kepala sekolah SDN 45/IV dengan pelaksana kegiatan pengabdian kepada masyarakat untuk menentukan hal-hal yang berkaitan dengan kegiatan pengabdian kepada masyarakat yang akan dilakukan seperti tempat kegiatan, jumlah peserta, serta sarana dan prasarana yang dibutuhkan.

2) Menentukan tempat pelaksanaan kegiatan

Pada tahap selanjutnya yakni menentukan tempat kegiatan yang akan digunakan sebagai tempat pelaksanaan kegiatan sosialisasi, tempat tersebut akan digunakan sebagai tempat untuk menyampaikan materi sosialisasi mengenai *malware* di SDN 45/IV Jambi

3) Menentukan waktu kegiatan dan penyusunan materi

Tahap selanjutnya yakni menentukan waktu untuk melakukan pelaksanaan kegiatan pengabdian masyarakat, Dimana waktunya yang digunakan selama kegiatan berlangsung yakni selama 3 jam dalam 1 kali pertemuan yang meliputi materi tentang bahaya *malware*.

b. Tahap penyuluhan

Tahap penyuluhan pengabdian kepada masyarakat menggunakan beberapa metode seperti sosialisasi, simulasi, dan tanya jawab.

1) Metode sosialisasi

Metode sosialisasi merupakan tahapanpenyampain materi sosialisasi yakni tentang *malware*, hal ini meliputi tentang pengertian, jenis-jenis, dan cara pencegahannya.

2) Metode simulasi

Metode simulsasi merupakan tahap dimana pemateri menyampaikan materi dengan memberikan contoh umum tentang *malware* kepada para peserta, agar para peserta mengetahui apa itu *malware* dan jenis-jenis nya serta cara mencegahnya.

3) Metode tanya jawab

Metode ini merupakan metode yang sangat penting bagi para peserta sosialisasi, karena metode ini merupkan tahap evaluasi untuk mengetahui sejauh mana para peserta memahami materi tentang *malware* tersebut.

3. Hasil dan Pembahasan

Kegiatan pengabdian kepada masyarakat (PKM) ini dilaksanakan dalam bentuk sosialisasi edukatif mengenai perangkat lunak berbahaya (*malware*) kepada siswa SDN 45/IV Kota Jambi kegiatan ini dilaksanakan pada tanggal 16 September 2025 dengan jumlah peserta sebanyak 32 orang.

Pada kegiatan sosialisasi tentang *malware* ini cukup membuat peserta menjadi antusias atas pemaparan yang dilakukan oleh tim pemateri sehingga materi dapat disampaikan dengan baik. Adapun tujuan dari kegiatan sosialisasi ini yaitu:

- 1) Peserta didik diharapkan mampu memahami konsep dasar tentang *malware*
Malware adalah singkatan dari *malicious software* atau perangkat lunak berbahaya. Secara sederhana, *malware* adalah program atau kode yang dibuat dengan tujuan merusak, mengganggu, atau mengambil alih sistem komputer, jaringan, maupun data penggunanya tanpa izin. *Malware* bekerja dengan cara memodifikasi *file*, mencuri data, atau melakukan eksekusi berbahaya tanpa sepengetahuan pengguna (Khalda, K., & Wibowo, D. K., 2025).
- 2) Peserta didik mampu mengenali jenis-jenis *malware*

Menurut Chandra et al., (2022), Jenis-jenis *malware* adalah sebagai berikut:

a. Virus

Virus adalah *malware* yang menempel (menyisip) pada *file* atau aplikasi tertentu, lalu menyebar ketika *file* tersebut dijalankan. Virus di komputer bekerja dengan cara menyisip pada *file* atau program tertentu, lalu aktif ketika *file* tersebut dijalankan, sehingga dapat merusak, mengubah, atau menghapus data.

b. Worm

Worm merupakan jenis *malware* yang mampu menggandakan dirinya dan menyebar secara otomatis melalui jaringan tanpa memerlukan interaksi pengguna, menyebabkan jaringan menjadi lambat atau bahkan berhenti berfungsi.

c. Trojan

Trojan horse atau kuda troya adalah *malware* yang menyamar sebagai aplikasi normal atau menarik, namun setelah dipasang dapat membuka akses bagi pelaku untuk mengendalikan perangkat korban atau memasukkan *malware* tambahan.

d. Ransomware

Ransomware merupakan *malware* yang mengunci atau *mengkripsi* data penting pada perangkat dan meminta tebusan agar data dapat dikembalikan. Dampaknya bisa berupa data tidak bisa dibuka atau bahkan hilang, kerugian finansial, dan lumpuhnya sistem yang sudah dicuri.

e. Spyware

Spyware adalah *malware* yang dirancang untuk merekam aktivitas pengguna secara diam-diam tanpa sepengetahuan pemilik perangkat, mulai dari ketikan pada keyboard (keylogging), riwayat pencarian, hingga data pribadi yang kemudian dikirimkan kepada pihak tidak bertanggung jawab.

f. Adware

Adware juga termasuk kategori *malware* karena menampilkan iklan secara berlebihan dan agresif, mengarahkan pengguna ke situs tertentu, serta mengumpulkan data perilaku pengguna tanpa izin, sehingga perangkat menjadi lemot dan boros kuota.

3) Peserta didik mengetahui bagaimana *malware* bisa masuk dan cara pencegahannya

Malware dapat masuk ke perangkat melalui berbagai celah kerentanan yang sering kali terjadi akibat kelalaian pengguna maupun lemahnya sistem keamanan. Salah satu cara paling umum adalah melalui tautan berbahaya yang diklik dari pesan, email, atau iklan pop-up yang tampak meyakinkan. Selain itu, *malware* juga dapat menyusup melalui aplikasi atau *file* yang diunduh dari situs tidak resmi, termasuk game bajakan, mod aplikasi, atau *file* yang nampak “gratis” namun sebenarnya disisipi kode berbahaya. Perangkat yang tidak diperbarui juga menjadi sasaran empuk karena memiliki celah keamanan yang belum ditutup, sehingga memudahkan *malware* untuk masuk tanpa disadari. Penggunaan Wi-Fi publik yang tidak aman, berbagi *file* melalui flashdisk, serta pemasangan aplikasi yang meminta izin berlebihan juga menjadi jalan masuk umum bagi berbagai jenis *malware*.

Untuk mencegahnya, pengguna perlu menerapkan kebiasaan digital yang aman, seperti berhati-hati terhadap tautan atau *file* yang mencurigakan, hanya mengunduh aplikasi dari sumber resmi, dan memastikan perangkat selalu diperbarui agar kerentanan sistem dapat tertutup dengan baik. Selain itu, penggunaan antivirus atau anti-*malware* yang tepercaya, pengaturan kata sandi yang kuat, serta membatasi izin aplikasi dapat secara signifikan menurunkan risiko infeksi. Pengguna juga perlu menghindari penggunaan Wi-Fi publik tanpa perlindungan dan melakukan pencadangan data secara rutin untuk mengantisipasi serangan seperti ransomware. Dengan menerapkan langkah-langkah ini, perangkat digital dapat terlindungi secara lebih optimal dari ancaman *malware* (Maslan, A., Annurullah Fajrin, A., & Dasa Putri, A., 2023).

Kegiatan sosialisasi ini berjalan sesuai dengan jadwal yang telah ditentukan sebagaimana ditunjukkan pada tabel 3.1.

Tabel 3.1 Jadwal Pelaksanaan Kegiatan Sosialisasi

Waktu	Kegiatan	Penanggung jawab
08.00	Pembukaan	Diah Aprilita Nizar
08.05	Tanya jawab awal	Seluruh tim sosialisasi
08.10	Penyampaian materi	Seluruh tim sosialisasi
08.45	<i>Ice breaking</i>	Diah, Rizal Kulfikri
08.50	Tanya jawab	Seluruh tim sosialisasi
09.00	Penutup	Diah Aprilita Nizar

Kegiatan diawali dengan sambutan dan penjelasan singkat tentang tujuan dari pelaksanaan kegiatan PKM. Pada sesi pembukaan, tim melakukan tanya jawab untuk mengetahui sejauh mana siswa-siswa tersebut memahami tentang istilah dari kata *malware*, hal ini menunjukkan bahwa peserta belum mengetahui apa itu *malware*, namun justru peserta hanya mengenal “virus komputer” saja dan belum memahami bentuk-bentuk *malware* lainnya seperti *trojan*, *worm*, *ransomware*, *adware* dan *spyware*.

Selanjutnya, pemeteri memaparkan materi menggunakan *power point* dan memberikan penjelasan mengenai *malware*, pemeteri menyampaikan materi dengan cara menganalogikan menjadi bahasa yang sederhana sehingga mampu dipahami oleh siswa sekolah dasar, kegiatan berjalan secara kondusif dan interaktif, yang mana para siswa diajak berdiskusi berdasarkan pengalaman pribadi saat menghadapi virus komputer atau perangkat yang melambat akibat terkena *malware*,

Berikutnya pemateri melakukan *ice breaking*, yaitu sedikit permainan kecil, hal ini bertujuan untuk merilekskan para siswa agar para siswa tidak merasa jenuh atau bosan ketika kegiatan sedang berlangsung.

Ketika merasa *ice breaking*nya sudah cukup, selanjutnya memasuki sesi tanya jawab, kegiatan ini berlangsung interaktif, dimana pada sesi ini tim memberikan kuis kecil dengan pemberian hadiah kepada peserta yang mampu menjawab pertanyaan. Hal ini bertujuan untuk mengetahui apakah para siswa sudah mengerti dan memahami tentang *malware*, cara ini sangat efektif meningkat motivasi dan antusiasme peserta terhadap kuis yang sedang berlangsung.

Berdasarkan evaluasi yang dilakukan melalui sesi tanya jawab interaktif, terlihat adanya peningkatan kesadaran dan pemahaman dasar yang cukup signifikan di kalangan siswa. Sebelum kegiatan dilaksanakan, sebagian besar siswa belum memahami bahwa perangkat lunak berbahaya (*malware*) dapat menyerang perangkat yang mereka gunakan setiap hari. Banyak di antara mereka yang masih bebas mengunduh aplikasi atau mengeklik tautan tanpa pertimbangan risiko, menunjukkan rendahnya kewaspadaan terhadap ancaman yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan informasi digital.

Setelah sesi penyampaian materi dan diskusi, beberapa perubahan positif mulai terlihat, antara lain:

- 1) Siswa mampu menyebutkan kembali jenis-jenis *malware* yang dijelaskan, seperti *virus*, *worm*, *trojan*, *ransomware*, *adware* dan *spyware*, serta menjelaskan secara sederhana bagaimana *malware* dapat masuk ke perangkat. Mereka juga dapat memberikan contoh aktivitas digital sehari-hari yang berpotensi mengundang *malware*.
- 2) Siswa mulai memahami bahwa mengeklik sembarang tautan, mengunduh game dari sumber yang tidak resmi, atau meminjamkan perangkat tanpa pengawasan dapat membuka peluang masuknya *malware*. Mereka menyadari perlunya bersikap hati-hati saat menggunakan perangkat digital.
- 3) Melalui contoh kasus nyata seperti perangkat yang tiba-tiba lambat, *file* hilang, atau akun diretas, siswa menunjukkan kekhawatiran yang lebih tinggi terhadap risiko tersebut. Hal ini menjadi motivasi bagi mereka untuk menerapkan perilaku yang lebih aman saat beraktivitas di internet.

Meskipun pemahaman awal sudah meningkat, penerapan langkah pencegahan secara konsisten masih membutuhkan arahan dari guru dan orang tua. Sosialisasi ini berhasil membangun pondasi kesadaran (*awareness*) yang penting sebelum diperkenalkannya kebijakan atau langkah keamanan yang lebih terstruktur bagi lingkungan sekolah.

4. Kesimpulan

Kegiatan sosialisasi pengenalan perangkat lunak berbahaya (*malware*) di SD Negeri 45/IV Kota Jambi berjalan dengan baik dan mencapai tujuan yang telah direncanakan. Melalui penyampaian materi interaktif, simulasi, dan sesi tanya jawab, siswa mampu memahami konsep dasar *malware* serta dampak yang dapat ditimbulkannya terhadap perangkat yang mereka gunakan sehari-hari. Antusiasme peserta terlihat dari keterlibatan aktif selama kegiatan, baik saat diskusi maupun saat menjawab pertanyaan pada sesi evaluasi.

Siswa yang sebelumnya hanya mengenal istilah “virus komputer” kini dapat menyebutkan beberapa jenis *malware* serta contoh aktivitas digital yang berisiko. Kegiatan ini juga berhasil meningkatkan kewaspadaan siswa terhadap tindakan sederhana yang dapat memicu infeksi *malware*, seperti mengunduh aplikasi sembarangan atau mengeklik tautan yang tidak dikenal. Dengan demikian, sosialisasi ini memberikan pondasi awal literasi keamanan digital yang sangat penting untuk melindungi data dan perangkat siswa.

Meskipun pemahaman dasar telah meningkat, pendampingan lanjutan dari guru dan orang tua tetap diperlukan agar perilaku aman dalam menggunakan internet dapat diterapkan secara konsisten. Secara keseluruhan, kegiatan pengabdian masyarakat ini memberikan kontribusi positif dalam menumbuhkan kesadaran dan pemahaman siswa sekolah dasar mengenai ancaman *malware* serta langkah pencegahannya sejak dini.

Dokumentasi



Referensi

- Asosiasi Penyelenggara Jasa Internet Indonesia. (2024). APJII: Jumlah pengguna internet Indonesia tembus 221 juta orang. APJII. <https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang>
- Chandra, S. D., Oktavianto, H., & Wardoyo, A. E. (2022). Klasifikasi malware menggunakan metode Convolutional Neural Network (CNN) berbasis website. *Jurnal Penelitian Teknologi Informasi dan Sains*. <https://doi.org/10.54066/jptis.v2i2.1931>
- Karim, W. N., & Kurniawan, A. J. (2025). SOSIALISASI PENGENALAN MALWARE DAN PENCEGAHANNYA BAGI MAHASISWA BARU PROGRAM STUDI SISTEM INFORMASI UIN SULTHAN THAHA SAIFUDDIN JAMBI. *Abdi Jurnal Publikasi*, 4(2), 23-27.
- Khalda, K., & Wibowo, D. K. (2025). Analisis perilaku malware menggunakan pendekatan analisis statis dan dinamis. *Jurnal Sains, Nalar, dan Aplikasi Teknologi Informasi*, 4(1), 1-8. <https://doi.org/10.20885/snati.v4.i1.1>
- Maslan, A., Fajrin, A. A., & Putri, A. D. (2023). Klasifikasi dan deteksi malware menggunakan variasi model algoritma machine learning. *JEPIN (Jurnal Edukasi dan Penelitian Informatika)*. <https://jurnal.untan.ac.id/index.php/jepin/article/view/87924>

- Napila, A., & Hidayat, A. (2025). SOSIALISASI PENGENALAN RANSOMWARE SEBAGAI PENINGKATAN KEAMANAN DATA SISWA DI SMK PANTI KARYA. *Abdi Jurnal Publikasi*, 3(6), 403-406.
- Satria, W., Prayoga, J., & Does, E. (2025). SOSIALISASI KEAMANAN SIBER BAGI PELAJAR DALAM MENGHADAPI ERA DIGITAL. *ABDI DALEM: Jurnal Pengabdian Kepada Masyarakat*, 2(1), 9-17.
- Schneier, B. (2019). Click Here to Kill Everybody: Security and Survival in a Hyper-connected World.
- Stallings, W., & Brown, L. (2020). Computer Security: Principles and Practice. Pearson Education.
- UNESCO. (2021). *Digital competencies and skills*. UNESCO. <https://www.unesco.org/en/digital-competencies-skills>
- UNICEF Office of Research - Innocenti. (2022). Digital Technology and Child Well-Being. UNICEF Innocenti. <https://www.unicef.org/innocenti/media/7081/file/WISH-Digital-Technology-and-Child-Wellbeing-2022.pdf>