LAPORAN PKM

WORKSHOP
1. PENGARUH DESAIN GRAFIS DALAM MEDIA PEMBELAJARAN
2. KESADARAN GURU TERHADAP KEAMANAN CYBER
BAGI GURU, TENAGA DAN STAFF PENDIDIKAN
LAB SCHOOL FIP UMJ

Oleh :

Mahbubul Wathoni, S.Si., M.Kom.
Dr. Yasin Efendi, S.Kom., M.Kom.
Ahmad Fikri Ardiansyah, S.T., M.T.I.
Sari Palestina, S.Kom., M.T.I.
Adi Alam, S.Kom., M.Si.
Rikaro Rahmadi, M.Kom.

FAKULTAS ILMU PENDIDIKAN
PRODI PENDIDIKAN TEKNOLOGI INFORMASI
UNIVERSITAS MUHAMMADIYAH JAKARTA
2021

HALAMAN PENGESAHAN

LAPORAN PENGABDIAN KEPADA MASYARAKAT

1. Judul	: **Workshop Pengaruh Desain Grafis dalam Media Pembelajaran dan Kesadaran Guru terhadap Keamanan Cyber**
2. Ketua Pelaksana	: Dr. Yasin Efendi, S.Kom, M.Kom
NIDN	: 0402117003
Pangkat/golongan	: Lektor / IIIC
Jabatan	: Ketua Pelaksana
3. Anggota Pelaksana Kegiatan	:
4. Lokasi Pelatihan/Workshop	: Auditorium FIP Universitas Muhammadiyah Jakarta
5. Jangka Waktu Pelatihan/workshop	: 1 hari
6. Biaya yang diperlukan	: Rp. 2.000.000,-
7. Sumber Dana	: Alokasi Dana PKM Prodi PTI FIP UMJ

Jakarta, 21 Desember 2021
Menyetujui
Ketua Prodi Pendidikan Teknologi Informasi

Mahbubul Wathoni, S.Si., M.Kom.

TIM PELAKSANA KEGIATAN WORKSHOP PENGABDIAN MASYARAKAT PENGARUH DESAIN GRAFIS DALAM MEDIA PEMBELAJARAN DAN KESADARAN GURU TERHADAP KEAMANAN CYBER BAGI GURU, TENAGA DAN STAFF PENDIDIKAN

1. Ketua Program Studi

Nama	: Mahbubul Wathoni, S.Si, M.Kom.
NIDN	: 0307088307:
Pangkat/Golongan	: Tenaga Pengajar
Jabatan	: Ketua Program Studi

2. Ketua Pelaksana

Nama	: Dr. Yasin Efendi, S.Kom., M.Kom
NIDN	: 0402117003
Pangkat/Golongan	: III/C
Jabatan	: Ketua Pelaksana

3. Anggota Pelaksana I

Nama	: Ahmad Fikri Ardiansyah, S.T., M.T.I.
NIDN	: 0309048405
Pangkat/golongan	: Tenaga Pengajar
Jabatan	: Dosen

4. Anggota Pelaksana II

Nama	: Sari Palestina, S.Kom., M.T.I.
NIDN	: 0319018704
Pangkat/golongan	: Tenaga Pengajar
Jabatan	: Dosen

5. Anggota Pelaksana III

Nama	: Adi Alam, S.Kom., M.Si..
NIDN	: 0311018005
Pangkat/golongan	: Tenaga Pengajar
Jabatan	**: Dosen**

6. Anggota Pelaksana IV

Nama	: Rikaro Rahmadi, M.Kom.
NIDN	: 0319018704
Pangkat/golongan	: Tenaga Pengajar
Jabatan	: Dosen

7. Anggota Pelaksana V

Nama	: Wahyu Iswantoro
NIM	: 2018880011
Pangkat/golongan	: -
Jabatan	: Mahasiswa

8. Anggota Pelaksana VI

Nama : Diah Budi Ratiningrum
NIM : 2018880010
Pangkat/golongan : -
Jabatan : Mahasiswa

9. Anggota Pelaksana VII

Nama : Mia Hariyani
NIM : 2018880008
Pangkat/golongan : -
Jabatan : Mahasiswa

10. Anggota Pelaksana VIII

Nama : Delina Syarfina
NIM : 2018880006
Pangkat/golongan : -
Jabatan : Mahasiswa

11. Anggota Pelaksana IX

Nama : Yoli Prastika Koto
NIM : 2018880007
Pangkat/golongan : -
Jabatan : Mahasiswa

`

12. Anggota Pelaksana X

Nama : Zihan Fauziah Rahmah
NIM : 2019880008
Pangkat/golongan : -
Jabatan : Mahasiswa

13. Anggota Pelaksana XI

Nama : Salsa Syahla Habibah
NIM : 2019880006
Pangkat/golongan : -
Jabatan : Mahasiswa

14. Anggota Pelaksana XII

Nama : Ratna Ayu Setyawati
NIM : 2019880012
Pangkat/golongan : -
Jabatan : Mahasiswa

15. Anggota Pelaksana XIII

Nama : Azriel Putra Junaedi
NIM : 2019880009
Pangkat/golongan : -
Jabatan : Mahasiswa

RINGKASAN
WORKSHOP PENGARUH DESAIN GRAFIS DALAM MEDIA PEMBELAJARAN DAN KESADARAN GURU TERHADAP KEAMANAN CYBER BAGI GURU, TENAGA DAN STAFF PENDIDIKAN

Sebagai salah satu bentuk kepedulian Lembaga Pengabdian kepada Masyarakat (LPM) dalam rangka untuk menjalin kerjasama dan untuk meningkatkan kualitas sumber daya manusia dalam penggunaan dan pengoperasian teknologi informasi/komputer dilingkungan SD Labschool FIP UMJ, maka Fakultas Ilmu Pendidikan Prodi Pendidikan Teknologi Informasi berinisiatif untuk melaksanakan suatu kegiatan Pengabdian Kepada Masyarakat dalam bentuk Workshop atau Pelatihan Teknologi Informasi dengan tema : Workshop Pengaruh Desain Grafis dalam Media Pembelajaran dan Kesadaran Guru terhadap Keamanan Cyber

Workshop Teknologi Informasi yang dilaksanakan di lingkungan SD Labschool FIP UMJ didasarkan pada pentingnya para guru, tenaga serta staff pendidikan dalam menguasai pengoperasian komputer dibidang grafis serta memberikan mereka pemahaman tentang keamanan cyber. Dengan dilaksanakannya program workshop ini diharapkan para guru, tenaga dan staff pendidikan dapat terampil mengoperasikan beberapa program komputer dibidang grafis dan kemamanan cyber.

Kegiatan workshop ini dilaksanakan pada Auditorium FIP Universitas Muhammadiyah Jakarta yang beralamat di Jalan KH Ahmad Dahlan Cireundeu Ciputat Timur, Kode Pos: 15419. Workshop dilaksanakan selama 1 (satu) hari yakni tanggal 17 Desember 2021. dengan peserta para guru, tenaga dan staff pendidikan dengan materi workshop adalah Pengaruh Desain Grafis dalam Media Pembelajaran dan Kesadaran Guru terhadap Keamanan Cyber. Di akhir Workshop para peserta diberikan tugas mendesain pembelajaran dan dari penilaian panitia, terdapat 3 (tiga) orang peserta dikukuhkan sebagai juara lomba 1,2 dan 3 serta 5 (lima) orang peserta lagi juara harapan.

Dengan adanya kegiatan workshop ini peserta sangat antusias berpartisipasi secara aktif ketika workshop dilaksanakan dan merasa sangat terbantu dalam pengembangan keterampilan kerja. Dari hasil evaluasi, secara umum workshop atau pelatihan yang telah dilaksanakan diantaranya meningkatnya keterampilan dan penguasaan para peserta workshop terhadap pengoperasian dan penggunaan teknologi informasi/komputer.

Berdasarkan hasil evaluasi yang dilakukan ternyata secara umum ada peningkatan pengetahuan peserta workshop. Diharapkan juga dari kegiatan ini para peserta dapat menularkan pengetahuan yang sudah didapatkan kepada guru, tenaga dan staff pendidiklan lainya di lingkungan SD Labschool FIP UMJ

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Ilahi Robbi, karena atas rahmat dan karuniaNya, Kami dapat menyelesaikan kegiatan workshop ini dengan judul workshop ***"Pengaruh Desain Grafis dalam Media Pembelajaran dan Kesadaran Guru terhadap Keamanan Cyber"*** yang dilaksanakan pada tanggal 17 Desember 2021 di Auditorium FIP UMJ dengan lancar.

Kegiatan workshop ini merupakan salah satu bagian dari Tri Dharma Perguruan Tinggi yang harus dilaksanakan oleh civitas akademika khususnya para dosen. Oleh karena itu, kami memberikan penghargaan yang setinggi-tingginya dan menyampaikan ucapan terima kasih banyak atas segala bantuan pihak-pihak terkait terutama kepada yang terhormat:

1. Mahbubul Wathoni,S.Si, M.Kom selaku Ketua Prodi Pendidikan Teknologi Informasi Universitas Muhammadiyah Jakarta;
2. Dindin Rosyidin, M.Pd, selaku Kepala Sekolah Lab School Biro Asesmen Profesi
3. Dosen dan Staff FIP UMJ Universitas Muhammadiyah Jakarta yang telah mambantu kelancaran pelaksanaan kegiatan pengabdian kepada masyarakat ini; dan

.

Akhir kata semoga kegiatan workshop ini dapat bermanfaat dan mudah-mudahan hasil kegiatan yang dilakukan ini akan terus berlanjut sesuai dengan tujuan pengabdian kepada masyarakat itu sendiri.

Jakarta, Desember 2021

Ketua Pelaksana

Dr. Yasin Efendi, M.Kom.

DAFTAR ISI

BAB I
PENDAHULUAN

1. Analisis Situasi

Perkembangan teknologi informasi dan komunikasi terus berkembang pesat dan telah merubah banyak cara kerja masyarakat. Salah satunya adalah pemanfaatan TIK dalam mempercepat proses pekerjaan dengan cara menyajikan suatu pekerjaan dalam bentuk grafis serta menjaga dan mencegah penyalahgunaan akses maupun pemanfaatan data dalam sistem Teknologi Informasi dari seseorang yang tidak memiliki hak untuk mengakses maupun memanfaatkan data dalam sistem tersebut.

Wilayah DKI Jakarta beserta wilayah-wilayah penyangganya seperti Tangerang Selatan dengan kemajuan teknologi Informasi menuntut masyarakatnya untuk dapat mengimbangi kemajuan teknologi dan cara kerja tersebut. Seperti halnya SD Lab Schoool FIP UMJ yang berlokasi di Cirendeu, Ciputat, perbatasan antara DKI Jakarta dan Tangerang Selatan, para guru, tenaga dan staff pendidikan diharapkan juga dapat mengikuti perkembangan teknologi informasi, dan alangkah lebih baiknya lagi jika menguasainya. Para guru, tenaga dan staff pendidiklan yang dalam hal ini dirasa perlu untuk ditingkatkan kemampuannya dalam menggunakan dan mengoperasikan peralatan teknologi infromasi/komputer. Dikarenakan dalam kegiatan sehari-hari di lingkungan Sekolah Dasar terutama dimasa pandemi ini diperlukan penguasaan dan keterampilan dalam menggoperasikan dan memakai program aplikasi grafis beserta keamanan cybernya.

Sebagai salah satu bentuk kepedulian Lembaga Penelitian dan Pengabdian kepada Masyarakat (LPPM) dalam rangka untuk mejalin kerjasama dan untuk meningkatkan kualitas sumber daya manusia dalam penggunaan dan pengoperasian teknologi informasi/komputer dilingkungan SD Lab Schoool, maka Prodi Pendidikan Teknologi Informasi merasa perlu dan berinisiatif untuk melaksanakan suatu kegiatan Pengabdian Kepada Masyarakat dalam bentuk workshop Teknologi Informasi bagi para guru, tenaga dan staff pendidikan.

2. Identifikasi dan Perumusan Masalah

Berdasarkan uraian di atas, beberapa masalah yang dapat penulis rumuskan adalah sebagai berikut :

1. Bagaimana edukasi visual di Lab School FIP UMJ?
2. Bagaimana penggunaan Comics dan Carton Maker?
3. Apa yang dikerjakan Cyber Security?

3. Tujuan

Kegiatan ini bertujuan untuk dapat :

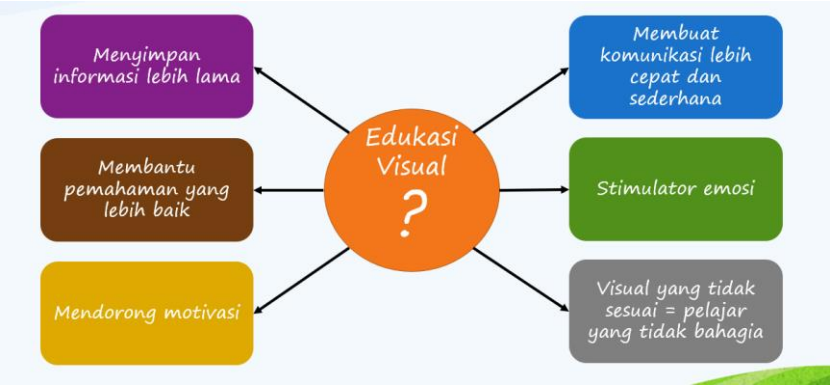
1. Mengetahui edukasi visual di Lab School FIP UMJ.
2. Mengetahui Penggunaan Comics dan Carton Maker.
3. Mengetahui hal-hal apa saja yang dikerjakan di Cyber Security.

4. Manfaat

Kegiatan ini diharapkan bermanfaat bagi para peserta workshop, rekan sejawat peserta, maupun masyarakat luas melalui perantara peserta yang sudah dilatih, serta diharapkan minat para guru, tenaga dan staff pendidikan untuk mempelajari teknologi informasi dan komunikasi semakin meningkat setelah dilakukan workshop ini

BAB II
TINJAUAN PUSTAKA

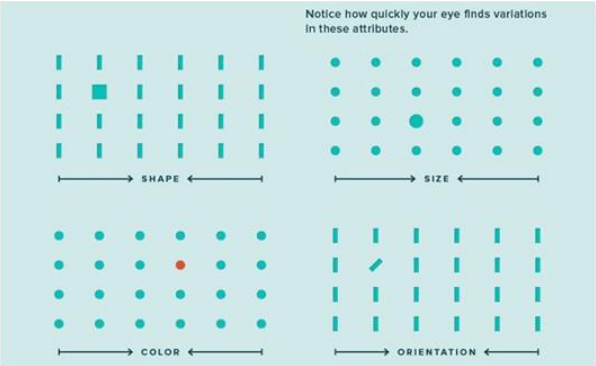
2.1 Desain Grafis



Gambar adalah cara paling sederhana dan paling efektif untuk memastikan bahwa informasi disimpan sebagai memori jangka panjang. Menurut Dr. Lynell Burmark, (seorang konsultan Pendidikan), memori jangka pendek kita dapat memproses kata-kata dan dapat menyimpan sekitar tujuh bit informasi, sementara gambar langsung diproses oleh memori jangka panjang (relatif sulit terlupakan)

Informasi berbasis teks yang disajikan dalam butir/bullet dapat lebih mudah untuk dimengerti daripada yang bulky, namun informasi yang sama dalam bentuk gambar atau video dapat diproses lebih cepat (Visual Teaching Alliance)

Visual membantu pelajar dalam memahami suatu konsep dengan lebih mudah dengan merangsang imajinasi dan mempengaruhi kemampuan kognitif. Selain itu, bahasa visual juga diketahui memiliki potensi "peningkatan kapasitas" yang terdiri dari menyerap, memahami, dan menganalisis informasi baru. Misalnya, infografis di bawah ini menunjukkan bagaimana kita telah diprogram untuk secara otomatis menafsirkan hubungan antara objek yang memastikan pemahaman instan dengan mudah:



Emosi dan informasi visual diproses di bagian yang sama dari otak manusia. Rangsangan visual dan respons emosional dihubungkan dengan cara yang sederhana dan keduanya bersama-sama menghasilkan apa yang kita sebut kenangan. Oleh karena itu, gambar yang kuat dan metafora visual menciptakan kesan yang kuat dan kenangan "abadi".

Sebagian siswa mungkin masih berjuang dengan beberapa mata pelajaran tertentu, karena mereka menganggapnya tidak menarik dan karenanya kurang termotivasi untuk melakukan upaya yang diperlukan. Pembelajaran melalui pendekatan berbasis gambar, video, chart, dll yang menarik dan relevan dapat membantu pelajar dalam melawan kebosanan serta memotivasi mereka dalam berusaha memahami suatu pelajaran dengan lebih baik.

Aspek positif dari visual hanya berlaku jika digunakan dengan tepat. Kualitas dan relevansi visual sangat penting, misalnya jika anda memiliki bahan ajar dalam bentuk gambar, chart, dan video yang menarik, namun dalam resolusi yang rendah (pixelated) maka besar kemungkinan materi tersebut akan gagal dalam menyampaikan pesan/tujuannya sehingga membuat pelajar kehilangan minat. Terlepas dari kualitas yang buruk, jika alat bantu visual tersebut bersifat generik dan gagal menjelaskan subjek dengan cara yang spesifik dan jelas, maka hal itu juga dapat "menghilangkan" minat pelajar.

A. Comics and Cartoon Maker(tm)

Comica adalah aplikasi gratis dan mudah digunakan yang mengubah foto menjadi komik/kartun. Anda dapat memilih gambar apa pun dari galeri Anda, atau mengambil yang baru melalui aplikasi. Setelah memilih filter, Anda dapat menambahkan balon ucapan untuk mendapatkan "efek komik" yang lebih meyakinkan. Ini adalah cara termudah untuk "membuat kartun diri sendiri" yang dapat Anda temukan secara online.

Bagaimana cara kerjanya?

* Unduh Comika
* Pilih opsi - ambil foto atau jelajahi galeri Anda
* Pilih efek foto yang paling sesuai dengan kartun yang baru Anda buat
* Tambahkan balon ucapan di gambar
* Simpan dan bagikan dengan teman-teman Anda

Comica juga merupakan pencipta meme yang sempurna. Menambahkan balon ucapan dalam gambar sekarang dimungkinkan dengan beberapa gesekan dan sedikit kreativitas.

Mengapa memilih Komika?

- Mudah digunakan
- Aplikasi ini ringan dan berjalan dengan lancar di ponsel apa pun
- Efek komik yang terlihat sah
- Anda dapat membuat meme Anda sendiri

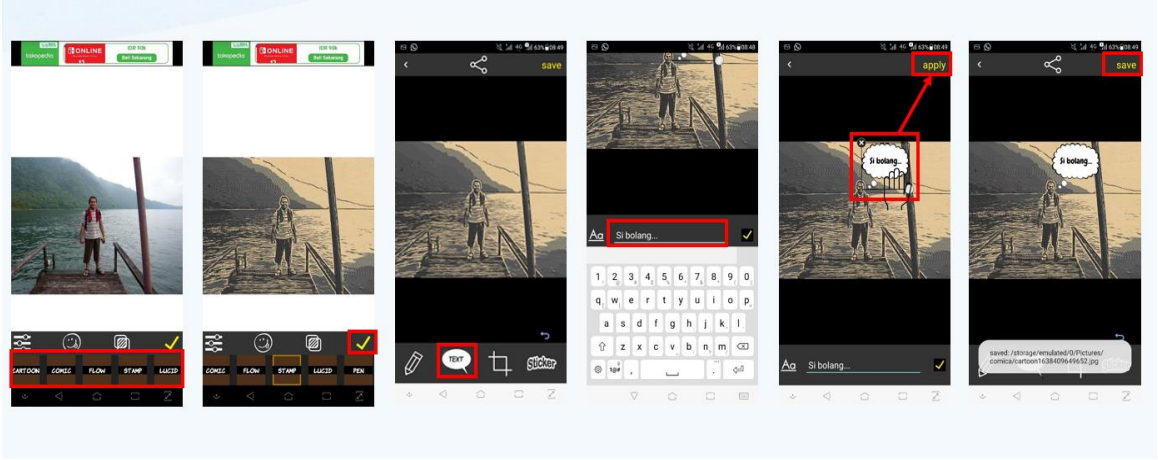
- Comika adalah aplikasi gratis

Aplikasi foto komik ini dimaksudkan agar mudah digunakan dan desainnya yang sederhana menjamin pengalaman pengguna yang luar biasa. Selain itu, ini berjalan dengan ringan dan bahkan smartphone yang lebih tua tidak akan memiliki masalah dengannya. Opsi "foto ke kartun" gratis, serta balon ucapan, tetapi jika Anda ingin membawa sesuatu ke tingkat berikutnya, Anda dapat membeli fitur tambahan dari bagian "Penjualan Besar". Apakah Anda seorang "pemboros besar"? Bahkan jika tidak, Anda pasti cocok untuk sepenuhnya menikmati foto ini ke aplikasi komik.

Apakah Anda ingin bersenang-senang dengan teman-teman Anda atau Anda hanya seorang pecinta komik yang mencari aplikasi gratis "kartun sendiri", Comica pasti layak untuk diunduh. Dapatkan, coba, dan nikmati sendiri.

1. Antarmuka

2. Efek Gambar



3. Template Layout

2.2 Keamanan Cyber

Module Flow

1. Information Security Overview
2. Cyber Kill Chain Concepts
3. Hacking Concepts
4. Ethical Hacking Concepts
5. Information Security Controls
6. Information Security Laws and Standards



Elements of Information Security

Information security is a state of well-being of information and infrastructure in which the possibility of **theft, tampering,** and **disruption of information and services** is low or tolerable

Confidentiality	Assurance that the information is accessible only to those **authorized to have access**
Integrity	The **trustworthiness of data or resources** in terms of preventing improper or unauthorized changes
Availability	Assurance that the systems responsible for delivering, storing, and processing information are accessible when **required by the authorized users**
Authenticity	Refers to the characteristic of a communication, document, or any data that ensures the **quality of being genuine**
Non-Repudiation	A **guarantee** that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message

Motives, Goals, and Objectives of Information Security Attacks

Attacks = Motive (Goal) + Method + Vulnerability

- A motive originates out of the notion that the **target system stores or processes** something valuable, and this leads to the threat of an attack on the system
- Attackers try various tools and attack techniques to **exploit vulnerabilities** in a computer system or its security policy and controls in order to fulfil their motives

Motives behind information security attacks

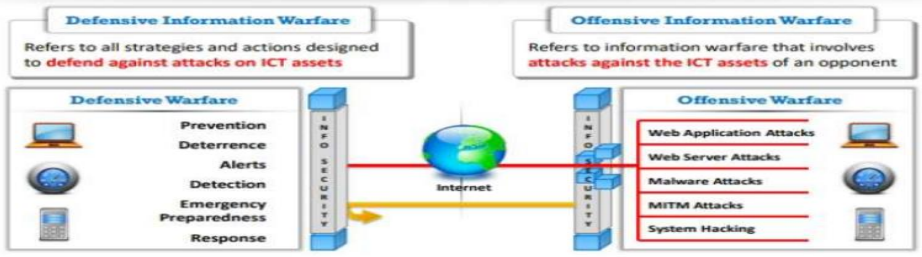
- Disrupting business continuity
- Stealing information and manipulating data
- Creating fear and chaos by disrupting critical infrastructures
- Causing financial loss to the target
- Propagating religious or political beliefs
- Achieving a state's military objectives
- Damaging the reputation of the target
- Taking revenge
- Demanding ransom

Classification of Attacks

Passive Attacks	• Passive attacks do not tamper with the data and involve intercepting and **monitoring network traffic** and data flow on the target network • Examples include sniffing and eavesdropping
Active Attacks	• Active attacks tamper with the data in transit or **disrupt the communication** or services between the systems to bypass or break into secured systems • Examples include DoS, Man-in-the-Middle, session hijacking, and SQL injection
Close-in Attacks	• Close-in attacks are performed when the attacker is in close physical proximity with the target system or network in order to gather, modify, or **disrupt access** to information • Examples include social engineering such as eavesdropping, shoulder surfing, and dumpster diving
Insider Attacks	• Insider attacks involve using privileged access to **violate rules** or intentionally cause a threat to the organization's information or information systems • Examples include theft of physical devices and planting keyloggers, backdoors, and malware
Distribution Attacks	• Distribution attacks occur when attackers **tamper with hardware** or **software** prior to installation • Attackers tamper with the hardware or software at its source or in transit

Information Warfare

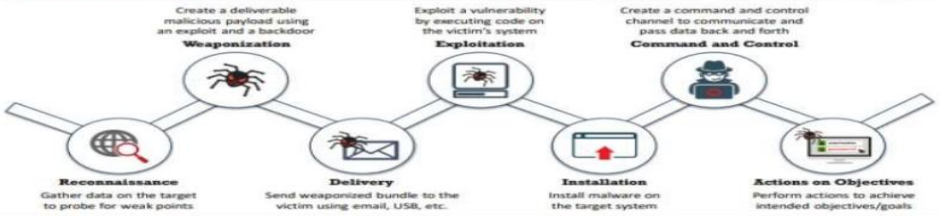
- The term information warfare or InfoWar refers to the **use of information and communication technologies (ICT)** to gain competitive advantages over an opponent



Module Flow

Cyber Kill Chain Methodology

- The cyber kill chain methodology is a component of intelligence-driven defense for the identification and **prevention of malicious intrusion activities**
- It provides greater insight into attack phases, which helps security professionals to understand the **adversary's tactics, techniques, and procedures beforehand**



Tactics, Techniques, and Procedures (TTPs)

The term Tactics, Techniques, and Procedures (TTPs) refers to the **patterns of activities and methods** associated with specific threat actors or groups of threat actors

Tactics

- "Tactics" are the guidelines that describe the **way an attacker performs the attack** from beginning to the end
- This guideline consists of the various **tactics for information gathering** to perform initial exploitation, privilege escalation, and lateral movement, and to deploy measures for persistent access to the system and other purposes

Techniques

- "Techniques" are the **technical methods used by an attacker** to achieve intermediate results during the attack
- These techniques include **initial exploitation**, setting up and maintaining **command and control channels**, accessing the target infrastructure, covering the tracks of data exfiltration, and others

Procedures

- "Procedures" are **organizational approaches that threat actors follow** to launch an attack
- The number of **actions usually differs** depending on the objectives of the procedure and threat actor group

Adversary Behavioral Identification

- Adversary behavioral identification involves the **identification of the common methods** or techniques followed by an adversary to launch attacks on or to penetrate an organization's network
- It gives the security professionals insight into **upcoming threats and exploits**

Adversary Behaviors

1 Internal Reconnaissance	4 Use of Command-Line Interface	7 Use of DNS Tunneling
2 Use of PowerShell	5 HTTP User Agent	8 Use of Web Shell
3 Unspecified Proxy Activities	6 Command and Control Server	9 Data Staging

Indicators of Compromise (IoCs)

- Indicators of Compromise (IoCs) are the **clues, artifacts,** and **pieces of forensic data** found on the network or operating system of an organization that indicate a potential intrusion or malicious activity in the organization's infrastructure
- IoCs are not intelligence, although they do **act as a good source of information** regarding the threats that serve as data points in the intelligence process
- Security professionals need to **perform continuous monitoring** of IoCs to effectively and efficiently detect and **respond to evolving cyber threats**

Categories of Indicators of Compromise

- Understanding IoCs helps security professionals to **quickly detect the threats** against the organization and protect the organization from evolving threats

For this purpose, IoCs are divided into four categories:

Email Indicators	Network Indicators	Host-Based Indicators	Behavioral Indicators
• Email indicators are used to send malicious data to the target organization or individual • Examples include the sender's email address, email subject, and attachments or links	• Network indicators are useful for command and control, malware delivery, identifying the operating system, and other tasks • Examples include URLs, domain names, and IP addresses	• Host-based indicators are found by performing an analysis of the infected system within the organizational network • Examples include filenames, file hashes, registry keys, DLLs, and mutex	• Behavioral indicators of compromise are used to identify specific behavior related to malicious activities • Examples of behavioral indicators include document executing PowerShell script, and remote command execution

Module Flow

1. Information Security Overview
2. Cyber Kill Chain Concepts
3. Hacking Concepts
4. Ethical Hacking Concepts
5. Information Security Controls
6. Information Security Laws and Standards



What is Hacking?

- Hacking refers to **exploiting system vulnerabilities and compromising security controls** to gain unauthorized or inappropriate access to a system's resources
- It involves **modifying system or application features** to achieve a goal outside of the creator's original purpose
- Hacking can be used to steal and redistribute intellectual property, leading to **business loss**

Who is a Hacker?

01

An intelligent individual with **excellent computer skills** who can create and explore computer software and hardware

02

For some hackers, **hacking is a hobby** to see how many computers or networks they can compromise

03

Some hackers' intentions can either be to gain knowledge or to **probe and do illegal things**

Some hack with **malicious intent** such as to steal business data, credit card information, social security numbers, email passwords, and other sensitive data

Hacker Classes

01 Black Hats

Individuals with extraordinary computing skills; they resort to malicious or destructive activities and are also known as crackers

02 White Hats

Individuals who use their professed hacking skills for defensive purposes and are also known as security analysts. They have permission from the system owner

03 Gray Hats

Individuals who work both offensively and defensively at various times

04 Suicide Hackers

Individuals who aim to bring down the critical infrastructure for a "cause" and are not worried about facing jail terms or any other kind of punishment

05 Script Kiddies

An unskilled hacker who compromises a system by running scripts, tools, and software that were developed by real hackers

06 Cyber Terrorists

Individuals with wide range of skills who are motivated by religious or political beliefs to create fear through the large-scale disruption of computer networks

07 State-Sponsored Hackers

Individuals employed by the government to penetrate and gain top-secret information from and do damage to the information systems of other governments

08 Hacktivist

Individuals who promote a political agenda by hacking, especially by defacing or disabling websites

Hacking Phase: Reconnaissance

- Reconnaissance refers to the preparatory phase where an **attacker seeks to gather information** about a target prior to launching an attack
- This information could be the future point of return, noted for ease of entry for an attack, when more about the **target is known on a broad scale**
- The reconnaissance **target range** may include the target organization's clients, employees, operations, network, and systems

Reconnaissance Types

Passive Reconnaissance

- Passive reconnaissance involves acquiring information **without directly interacting with the target**
- For example, searching public records or news releases

Active Reconnaissance

- Active reconnaissance involves **directly interacting with the target by any means**
- For example, telephone calls to the target's help desk or technical department

Hacking Phase: Scanning

Pre-attack Phase	Scanning refers to the pre-attack phase when the attacker **scans the network** for specific information based on information gathered during reconnaissance
Port Scanner	Scanning can include the use of dialers, **port scanners**, network mappers, ping tools, and vulnerability scanners
Extract Information	Attackers extract information such as **live machines**, port, port status, OS details, device type, and **system uptime** to launch attack

Hacking Phase: Gaining Access

1. Gaining access refers to the point where the attacker obtains access to the **operating system or applications** on the target computer or network
2. The attacker can gain access at the **operating system, application,** or **network levels**
3. The attacker can **escalate privileges** to obtain complete control of the system. In this process, the target's connected intermediate systems are also compromised
4. Examples include **password cracking**, buffer overflows, denial of service, and **session hijacking**

Hacking Phase: Maintaining Access

Maintaining access refers to the phase when the attacker tries to retain their **ownership of the system**

Attackers may prevent the system from being owned by other attackers by securing their exclusive access with **backdoors**, **rootkits**, or **trojans**

Attackers can upload, download, or **manipulate data**, applications, and configurations on the **owned system**

Attackers use the compromised system to **launch further attacks**

Hacking Phase: Clearing Tracks

1. Clearing tracks refers to the activities carried out by an attacker to **hide malicious acts**

2. The attacker's intentions include obtaining **continuing access** to the victim's system, remaining **unnoticed and uncaught**, and deleting evidence that might lead to their prosecution

3. The attacker overwrites the server, system, and application logs to **avoid suspicion**

Attackers always cover their tracks to hide their identity

Module Flow

1. **Information Security Overview**
2. **Cyber Kill Chain Concepts**
3. **Hacking Concepts**
4. **Ethical Hacking Concepts**
5. **Information Security Controls**
6. **Information Security Laws and Standards**

What is Ethical Hacking?

- Ethical hacking involves the use of hacking tools, tricks, and techniques to **identify vulnerabilities** and ensure system security

- It focuses on simulating the techniques used by attackers to **verify the existence of exploitable vulnerabilities** in a system's security

- Ethical hackers perform security assessments for an organization **with the permission of concerned authorities**

Why Ethical Hacking is Necessary

To beat a hacker, you need to think like one!

Ethical hacking is necessary as it **allows for counter attacks against malicious hackers** through anticipating the methods used to break into the system

Reasons why organizations recruit ethical hackers

- To **prevent hackers** from gaining access to the organization's information systems
- To **uncover vulnerabilities** in systems and explore their potential as a security risk
- To analyze and **strengthen an organization's security posture**, including policies, network protection infrastructure, and end-user practices
- To provide adequate preventive measures in order to **avoid security breaches**
- To help **safeguard customer data**
- To **enhance security awareness** at all levels in a business

Why Ethical Hacking is Necessary (Cont'd)

Ethical Hackers Try to Answer the Following Questions

1. What can an intruder see on the **target system**? (Reconnaissance and Scanning phases)
2. What can an **intruder do** with that information? (Gaining Access and Maintaining Access phases)
3. Does anyone at the target organization **notice the intruders' attempts** or successes? (Reconnaissance and Covering Tracks phases)
4. Are all **components of the information system** adequately protected, updated, and patched?
5. How much time, effort, and money are required to obtain **adequate protection**?
6. Are the **information security measures** in compliance with legal and industry standards?

Scope and Limitations of Ethical Hacking

Scope

- Ethical hacking is a crucial component of **risk assessment, auditing, counter fraud**, and information systems security **best practices**
- It is used to **identify risks** and highlight **remedial actions**. It also reduces ICT costs by resolving vulnerabilities

Limitations

- Unless the businesses already know what they are looking for and why they are **hiring an outside vendor to hack systems** in the first place, chances are there would not be much to gain from the experience
- An ethical hacker can only help the organization to better **understand its security system**; it is up to the organization to **place the right safeguards** on the network

Skills of an Ethical Hacker

1 Technical Skills

- In-depth **knowledge of major operating environments** such as Windows, Unix, Linux, and Macintosh
- In-depth **knowledge of networking** concepts, technologies, and related hardware and software
- A **computer expert** adept at technical domains
- **Knowledgeable about security areas** and related issues
- **"High technical" knowledge** for launching sophisticated attacks

2 Non-Technical Skills

- The **ability to learn** and adopt new technologies quickly
- **Strong work ethics** and good problem solving and communication skills
- Committed to the **organization's security policies**
- An awareness of **local standards and laws**

Module Flow

1. **Information Security Overview**
2. **Cyber Kill Chain Concepts**
3. **Hacking Concepts**
4. **Ethical Hacking Concepts**
5. **Information Security Controls**
6. **Information Security Laws and Standards**

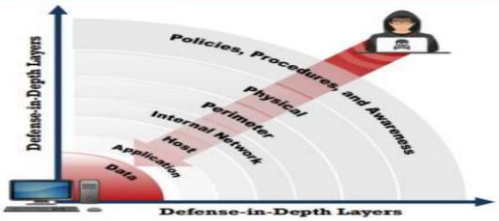
Information Assurance (IA)

- IA refers to the assurance that the **integrity, availability, confidentiality,** and **authenticity** of information and information systems is protected during the usage, processing, storage, and transmission of information
- Some of the processes that help in achieving information assurance include:

1. Developing local policy, process, and guidance
2. Designing network and user authentication strategies
3. Identifying network vulnerabilities and threats
4. Identifying problem and resource requirements
5. Creating plans for identified resource requirements
6. Applying appropriate information assurance controls
7. Performing certification and accreditation
8. Providing information assurance training

Defense-in-Depth

- Defense-in-depth is a security strategy in which **several protection layers** are placed throughout an information system
- It helps to **prevent direct attacks** against the system and its data because a break in one layer only leads the attacker to the next layer



Risk Management

- Risk management is the process of **reducing and maintaining risk at an acceptable level** by means of a well-defined and actively employed security program

Risk Management Phases

Risk Identification	**Identifies the sources**, causes, consequences, and other details of the internal and external risks affecting the security of the organization
Risk Assessment	**Assesses the organization's risk** and provides an estimate of the likelihood and impact of the risk
Risk Treatment	**Selects and implements appropriate controls** for the identified risks
Risk Tracking	**Ensures appropriate controls are implemented** to handle known risks and calculates the chances of a new risk occurring
Risk Review	**Evaluates the performance** of the implemented risk management strategies

Cyber Threat Intelligence

- Cyber Threat Intelligence (CTI) is defined as the **collection and analysis of information** about threats and adversaries and the drawing of patterns that provide the ability to make knowledgeable decisions for preparedness, prevention, and response actions against various cyber-attacks
- Cyber threat intelligence helps the organization to **identify and mitigate various business risks** by converting unknown threats into known threats; it helps in implementing various advanced and proactive defense strategies

Threat Modeling

Threat modeling is a **risk assessment approach** for analyzing the security of an application by capturing, organizing, and analyzing all the information that affects the security of an application

Threat Modeling Process

01	Identify Security Objectives	Helps to determine how much **effort needs to be put** toward subsequent steps
02	Application Overview	Identify the **components, data flows,** and trust boundaries
03	Decompose the Application	Helps to find more relevant and more **detailed threats**
04	Identify Threats	Identify threats relevant to the **control** scenario and context using the information obtained in steps 2 and 3
05	Identify Vulnerabilities	**Identify weaknesses** related to the threats found using **vulnerability categories**

Module Flow

1. Information Security Overview
2. Cyber Kill Chain Concepts
3. Hacking Concepts
4. Ethical Hacking Concepts
5. Information Security Controls
6. Information Security Laws and Standards



Payment Card Industry Data Security Standard (PCI DSS)

- The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary **information security standard for organizations** that handle cardholder information for major debit, credit, prepaid, e-purse, ATM, and POS cards
- PCI DSS **applies to all entities involved in payment card processing** — including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process, or transmit cardholder data

PCI Data Security Standard — High Level Overview

Build and Maintain a Secure Network	Implement Strong Access Control Measures
Protect Cardholder Data	Regularly Monitor and Test Networks
Maintain a Vulnerability Management Program	Maintain an Information Security Policy

https://www.pcisecuritystandards.org

Failure to meet the PCI DSS requirements may result in fines or the termination of payment card processing privileges

ISO/IEC 27001:2013

- ISO/IEC 27001:2013 specifies the requirements for **establishing**, **implementing**, **maintaining**, and continually improving an **information security management system** within the context of the organization
- It is intended to be suitable for several different types of use, including:

1. Use within organizations to formulate **security requirements** and **objectives**
2. Use within organizations to ensure that security risks are **cost-effectively managed**
3. Use within organizations to **ensure compliance with laws and regulations**
4. Definition of new **information security management processes**
5. Identification and clarification of existing **information security management processes**
6. Use by organization management to determine the **status of information security management activities**
7. Implementation of **business-enabling information security**
8. Use by organizations to provide relevant information about **information security** to customers

https://www.iso.org

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA's Administrative Simplification Statute and Rules

Electronic Transaction and Code Set Standards	Requires every provider who does business electronically to **use the same health care transactions**, **code sets**, and **identifiers**
Privacy Rule	Provides **federal protections for the personal health information** held by covered entities and gives patients an array of rights with respect to that information
Security Rule	Specifies a series of administrative, physical, and technical safeguards for covered entities to use to ensure the **confidentiality**, **integrity**, and **availability of electronically protected health information**
National Identifier Requirements	Requires that health care providers, health plans, and employers have standard national numbers that identify them attached to **standard transactions**
Enforcement Rule	Provides the standards for enforcing all the **Administration Simplification Rules**

https://www.hhs.gov

Sarbanes Oxley Act (SOX)

- Enacted in 2002, the Sarbanes-Oxley Act is designed to **protect investors and the public** by increasing the accuracy and reliability of corporate disclosures
- The key requirements and provisions of SOX are organized into **11 titles**:

Title I	**Public Company Accounting Oversight Board (PCAOB)** provides independent oversight of public accounting firms providing audit services ("auditors")
Title II	**Auditor Independence** establishes the standards for external auditor independence, intended to limit conflicts of interest and address new auditor approval requirements, audit partner rotation, and auditor reporting requirements
Title III	**Corporate Responsibility** mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports
Title IV	**Enhanced Financial Disclosures** describe enhanced reporting requirements for financial transactions, including off-balance-sheet transactions, pro-forma figures, and the stock transactions of corporate officers
Title V	**Analyst Conflicts of Interest** consist of measures designed to help restore investor confidence in the reporting of securities analysts
Title VI	**Commission Resources and Authority** defines practices to restore investor confidence in securities analysts

Sarbanes Oxley Act (SOX) (Cont'd)

Title VII	**Studies and Reports** includes the effects of the consolidation of public accounting firms, the role of credit rating agencies in the operation of securities markets, securities violations and enforcement actions, and whether investment banks assisted Enron, Global Crossing, or others to manipulate earnings and obfuscate true financial conditions
Title VIII	**Corporate and Criminal Fraud Accountability** describes specific criminal penalties for fraud by the manipulation, destruction, or alteration of financial records, or other interference with investigations while providing certain protections for whistle-blowers
Title IX	**White Collar Crime Penalty Enhancement** increases the criminal penalties associated with white-collar crimes and conspiracies. It recommends stronger sentencing guidelines and specifically adds the failure to certify corporate financial reports as a criminal offense
Title X	**Corporate Tax Returns** states that the Chief Executive Officer should sign the company tax return
Title XI	**Corporate Fraud Accountability** identifies corporate fraud and record tampering as criminal offenses and assigns them specific penalties. It also revises sentencing guidelines and strengthens their penalties. This enables the SEC to temporarily freeze large or unusual payments

https://www.sec.gov

The Digital Millennium Copyright Act (DMCA) and the Federal Information Security Management Act (FISMA)

The Digital Millennium Copyright Act (DMCA)

- The DMCA is a United States copyright law that implements two 1996 treaties of the **World Intellectual Property Organization** (WIPO)
- It **defines the legal prohibitions** against the circumvention of technological protection measures employed by copyright owners to protect their works, and against the removal or alteration of copyright management information

https://www.copyright.gov

Federal Information Security Management Act (FISMA)

- The FISMA provides a comprehensive framework for ensuring the **effectiveness of information security controls** over information resources that support Federal operations and assets
- It includes
  - Standards for categorizing information and information systems by mission impact
  - Standards for minimum security requirements for information and information systems
  - Guidance for selecting appropriate security controls for information systems
  - Guidance for assessing security controls in information systems and determining security control effectiveness
  - Guidance for security authorization of information systems

https://csrc.nist.gov

Cyber Law in Different Countries

Country Name	Laws/Acts	Website
United States	Section 107 of the Copyright Law mentions the doctrine of "fair use"	https://www.copyright.gov
	Online Copyright Infringement Liability Limitation Act	
	The Lanham (Trademark) Act (15 USC §§ 1051 - 1127)	https://www.uspto.gov
	The Electronic Communications Privacy Act	https://fas.org
	Foreign Intelligence Surveillance Act	https://fas.org
	Protect America Act of 2007	https://www.justice.gov
	Privacy Act of 1974	https://www.justice.gov
	National Information Infrastructure Protection Act of 1996	https://www.nrotc.navy.mil
	Computer Security Act of 1987	https://csrc.nist.gov
	Freedom of Information Act (FOIA)	https://www.foia.gov
	Computer Fraud and Abuse Act	https://energy.gov
	Federal Identity Theft and Assumption Deterrence Act	https://www.ftc.gov

Cyber Law in Different Countries (Cont'd)

Country Name	Laws/Acts	Website
Australia	The Trade Marks Act 1995	https://www.legislation.gov.au
	The Patents Act 1990	
	The Copyright Act 1968	
	Cybercrime Act 2001	
United Kingdom	The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002	https://www.legislation.gov.uk
	Trademarks Act 1994 (TMA)	
	Computer Misuse Act 1990	
China	Copyright Law of the People's Republic of China (Amendments on October 27, 2001)	http://www.npc.gov.cn
	Trademark Law of the People's Republic of China (Amendments on October 27, 2001)	
India	The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957	http://www.ipindia.nic.in
	Information Technology Act	https://www.meity.gov.in
Germany	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	https://www.cybercrimelaw.net

Cyber Law in Different Countries (Cont'd)

Country Name	Laws/Acts	Website
Italy	Penal Code Article 615 ter	https://www.cybercrimelaw.net
Japan	The Trademark Law (Law No. 127 of 1957), Copyright Management Business Law (4.2.2.3 of 2000)	https://www.iip.or.jp
Canada	Copyright Act (R.S.C., 1985, c. C-42), Trademark Law, Canadian Criminal Code Section 342.1	https://laws-lois.justice.gc.ca
Singapore	Computer Misuse Act	https://sso.agc.gov.sg
South Africa	Trademarks Act 194 of 1993	http://www.cipc.co.za
	Copyright Act of 1978	https://www.nlsa.ac.za
South Korea	Copyright Law Act No. 3916	https://www.copyright.or.kr
	Industrial Design Protection Act	https://www.kipo.go.kr
Belgium	Copyright Law, 30/06/1994	https://www.wipo.int
	Computer Hacking	https://www.cybercrimelaw.net
Brazil	Unauthorized modification or alteration of the information system	https://www.domstol.no
Hong Kong	Article 139 of the Basic Law	https://www.basiclaw.gov.hk

Module Summary

- This module discussed elements of information security, information security attacks, and information warfare
- It discussed cyber kill chain methodology, TTPs, and IoCs in detail
- It also discussed hacking concepts, types, and phases
- This module also covered ethical hacking concepts such as the scope and limitations of ethical hacking, skills, and other pertinent information in detail
- It discussed information security controls such as defense-in-depth, risk management, cyber threat intelligence, threat modeling, incident management process, and AI and ML
- This module ended with a detailed discussion of various information security acts and laws from around the world
- The next module will go into detail about how attackers, as well as ethical hackers and pen testers, perform footprinting to collect information about the target of an evaluation before an attack or audit

Cyber Law in Different Countries (Cont'd)

Country Name	Laws/Acts	Website
Italy	Penal Code Article 615 ter	https://www.cybercrimelaw.net
Japan	The Trademark Law (Law No. 127 of 1957), Copyright Management Business Law (4.2.2.3 of 2000)	https://www.iip.or.jp
Canada	Copyright Act (R.S.C., 1985, c. C-42), Trademark Law, Canadian Criminal Code Section 342.1	https://laws-lois.justice.gc.ca
Singapore	Computer Misuse Act	https://sso.agc.gov.sg
South Africa	Trademarks Act 194 of 1993	http://www.cipc.co.za
	Copyright Act of 1978	https://www.nlsa.ac.za
South Korea	Copyright Law Act No. 3916	https://www.copyright.or.kr
	Industrial Design Protection Act	https://www.kipo.go.kr
Belgium	Copyright Law, 30/06/1994	https://www.wipo.int
	Computer Hacking	https://www.cybercrimelaw.net
Brazil	Unauthorized modification or alteration of the information system	https://www.domstol.no
Hong Kong	Article 139 of the Basic Law	https://www.basiclaw.gov.hk

BAB III
PELAKSANAAN KEGIATAN

A. Realisasi Pemecahan Masalah

Persiapan Kegiatan Workshop

Sebelum kegiatan dilaksanakan maka dilakukan persiapan-persiapan sebagai berikut:

1. Melakukan studi pustaka tentang Pengaruh Desain Grafis dalam Media Pembelajaran dan Kesadaran Guru terhadap Keamanan Cyber yang perlu dikuasasi oleh para guru, tenaga dan staff pendidikan di lingkungan SD Lab School FIP UMJ.
2. Melakukan persiapan ruangan workshop dan peralatan TIK yang akan digunakan.
3. Melukan uji coba peralatan TIK sebelum dilakukan workshop
4. Menentukan waktu dan lama pelaksanaan kegiatan workshop bersama tim pelaksana.
5. Menentukan dan mempersiapkan materi workshop yang akan disampaikan.

Waktu & Tempat Pelaksanaan Kegiatan Workshop

Pelaksanaan kegiatan worksop ini dilaksanakan pada pada tanggal 17 Desember 2021. Kegiatan workshop terbagi 2 sesi, yaitu :

Sesi I : dimulai dari pukul 08.00 s.d pukul 12.00 tentang Pengaruh Desain Grafis dalam Media Pembelajaran dan

sesi ke II : dimulai dari pukul 13.00 s.d pukul 17.00 tentang Kesadaran Guru terhadap Keamanan Cyber yang perlu dikuasasi oleh para guru, tenaga dan staff pendidikan di lingkungan SD Lab School FIP UMJ.

Lokasi workshop bertempat di Auditorium FIP Universitas Muhammadiyah Jakarta

B. Khalayak Sasaran

Khalayak yang menjadi sasaran workshop ini adalah para Guru, Tenaga dan staff pendidikan SD Lab School FIP UMJ keseluruhnya berjumlah 84 (delapan puluh empat) Orang dibagi menjadi 2 sesi/tim.

C. Relevansi bagi Sasaran

Kegiatan workshop ini memiliki relevansi dengan kebutuhan para guru, tenaga dan staff pendidikan. Berdasarkan informasi dari temen sejawat di SD Labschool FIP UMJ, masih terdapat guru, tenga dan staff pendidikan yang belum sepenuhnya mampu mengoperasikan Desain Grafis. Hal tersebut juga selaras dengan permintaan dari pihak Lab School untuk melakukan workshop Desain Grafis dan Cyber Media.

D. Metoda

Teknik yang digunakan dalam menyampaikan materi workshop atau pelatihan adalah *workshop* (ceramah penyuluhan, praktek dan diskusi) dengan menggunakan alat bantu multimedia berupa laptop/PC, LCD proyektor dan modul materi workshop atau pelatihan.

E. Hasil Kegiatan

- Respon dari Peserta

Berdasarkan wawancara, tanya jawab dan pengamatan langsung selama kegiatan berlangsung, kegiatan pengabdian pada masyarakat ini memberikan hasil : Meningkatnya pemahaman dan keterampilan para guru, tenaga dan staff pendidikan dalam menggunakan desain grafis dan cyber security.

Dilihat dari aktivitas peserta di forum workshop atau pelatihan, maka terlihat respon para peserta sangat tinggi. Banyak di antara mereka yang bertanya dan kemudian terlibat dalam diskusi, dan kemudian menindak-lanjutinya dengan praktek materi yang mereka pertanyakan. Respon yang antusias kebanyakan muncul dari peserta yang pernah tahu namun belum tuntas atau masih ragu-ragu. Forum workshop atau pelatihan ini dijadikan ajang untuk bertanya hal-hal yang detail sifatnya.

Sedangkan para peserta yang belum tahu sama sekali atau belum pernah sama sekali menjalankan program ini cenderung pasif. Responnya yang mereka berikan sangat sedikit. Pada umumnya mereka terlihat takut-takut untuk bertanya. Namun ketika instruktur workshop atau pelatihan ini mendekat dan menanyakan kesulitan mereka secara personal,

mereka lebih terbuka dan mau mengutarakan keinginan mereka untuk mendapatkan bantuan. Sebenarnya ada banyak hal yang ingin mereka tanyakan.

Namun demikian secara umum dari raut muka mereka terlihat bahwa semua peserta memiliki semangat tinggi mengikuti latihan dan memiliki rasa ingin tahu yang besar. Sebagian di antara mereka menceriterakan bahwa sebenarnya ada diantara temen mereka, telah menguasai Desain Grafis dan pemahaman Keamanan Cyber namun mereka tidak pernah memiliki kesempatan untuk bertanya dan berlatih.

- Hambatan dan Kendala

Pada dasarnya pelaksanaan Pelatihan desain grafis dan keamanan cyber ini untuk Peningkatan Kemampuan para guru, tenaga dan staff pendidikan SD Lab Sachool FIP UMJ, namun demikian bilamana ditelaah lebih lanjut, masih ada beberapa aspek yang memiliki kekurangan dan bisa diperbaiki untuk hasil yang lebih maksimal. Berbagai kekurangan itu terangkum dalam uraian sebagai berikut :

1. Ketersediaan alat

Masalah klasik yang selalu muncul dalam pembelajaran berbasis komputer adalah keterbatasan alat, baik hardware maupun software-nya. .

2. Keaneka-ragaman Kemampuan Awal Peserta

Para peserta aktif workshop atau pelatihan ini ternyata memiliki kemampuan awal yang berbeda-beda. Ada yang sudah tingkat lanjut (mahir) dan ada pula yang masih tingkat dasar. Kebanyakan diantara mereka memiliki pengetahuan yang masih dasar, bahkan ada di antara mereka yang masih sangat awam. Kondisi ini sangat mempengaruhi efisiensi waktu dan efektifitas pelaksanaan workshop atau pelatihan ini. Instruktur dituntut untuk lebih sabar dan memperlakukan para peserta kasus per kasus.

Metode pengajaran klasikal yang dirancang untuk workshop atau pelatihan ini pada prakteknya tidak bisa diterapkan secara massal. Sifat interaktif model pembelajaran komputer aplikatif semacam ini juga tidak bisa dimanfaatkan secara efektif. Setiap dialog box, pesan, perintah ataupun rekomendasi tertentu yang muncul dari sistem komputer tidak bisa ditindak-lanjuti sendiri oleh peserta workshop atau pelaihan. Penciptaan proses belajar yang mandiri tidak bisa diterapkan dalam forum ini. Oleh karena itu terpaksa cara belajar konvensional

kembali diterapkan. Bahkan pembimbingan secara personal terhadap peserta workshop atau pelatihan satu per satu mutlak diperlukan. Akibatnya waktu yang dialokasikan untuk workshop atau pelaihan ini (1 hari) terasa sangat kurang.

Selanjutnya tidak semua materi program workshop atau pelaihan ini dapat disampaikan secara tuntas. Sebenarnya masih banyak solusi alternatif untuk belajar Desain Grafis dan Cyber Security ini. Namun demikian oleh karena kondisi para peserta workshop atau pelaihan yang sangat beragam itu, maka kesemuan fasilitas belajar itu tidak bisa dilatihkan dalam forum ini.

BAB IV
PENUTUP

1. Kesimpulan

Berdasarkan hasil pelaksanaan kegiatan yang telah dilakukan, dapat ditarik beberapa simpulan sebagai berikut;

1) Edukasi Visual terbagi menjadi beberapa bagian diantaranya membuat komunikasi lebih cepat dan sederhana, stimulaltor emosi, visual yang tidak sesuai pelajar yang tidak bahagia, mendorong motivasi, menyimpan informasi lebih lama serta membantu pemahaman yang lebih

2) Pengunaan Comics dan Cartoon Maker terdiri dari beberapa langkah penting yaitu mula- mula lakukan unduh comika, setelah pengunduhan selesai lalu pilih opsi ambil photo atau jelajahi galeri anda, kemudian pilih efek foto yang paling sesuai dengan kartun yang baru anda buat, selanjutnya tambahkan balon ucapan digambar dan terakhir adalah simpan dan bagikan dengan rekan- rekan anda.

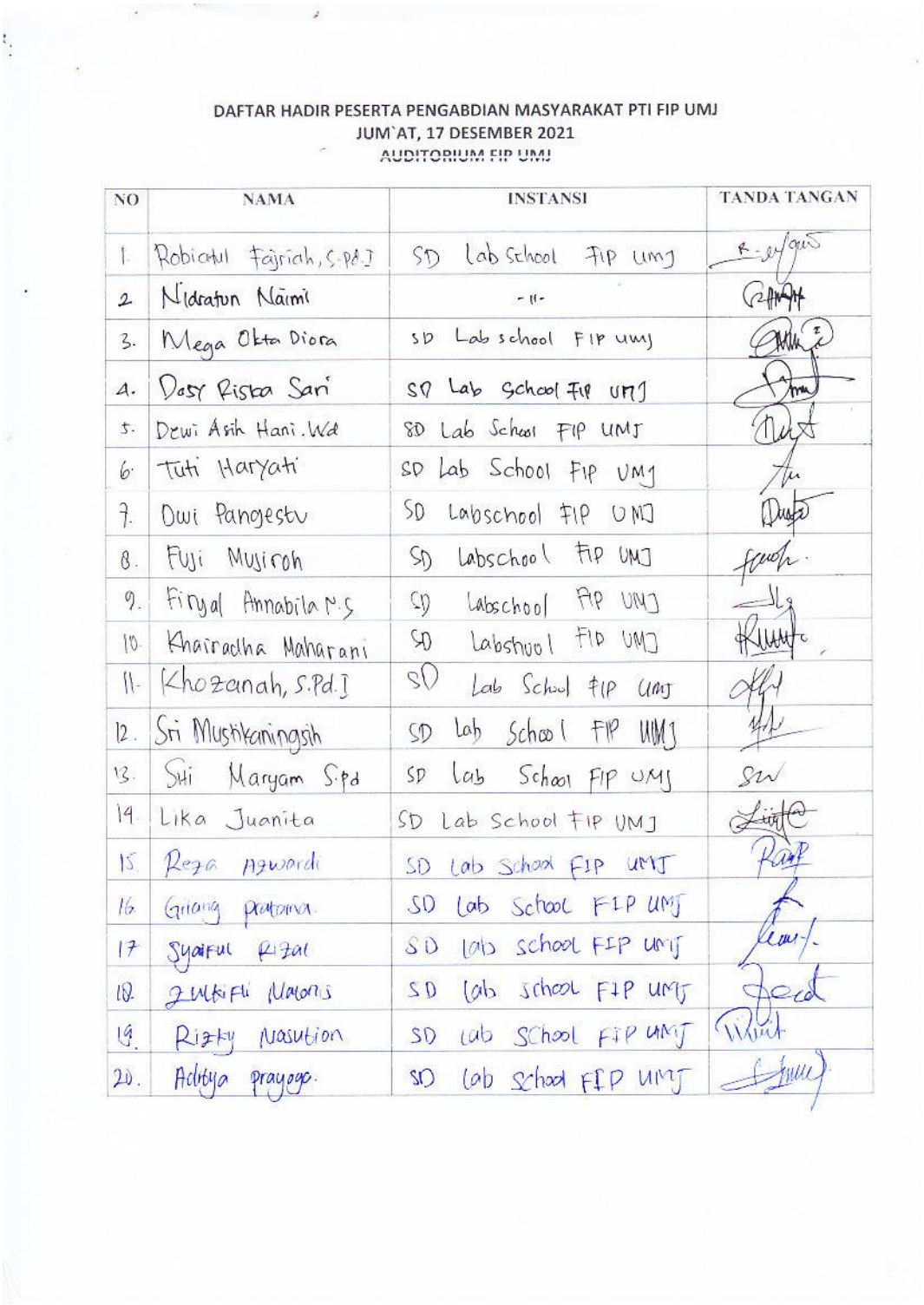
3) Yang dikerjakan Cyber Security adalah sebagai berikut melindungsi sistem komputer dari serangan atau akses ilegal, melindungi data perusahaan.

2. Saran dan Tindak Lanjut

Menutup laporan kegiatan Pengabdian pada Masyarakat ini perlu disampaikan bahwa untuk menyelenggarakan PKM dengan bentuk penyelenggaraan workshop Desain Grafis dan Cyber Security semacam ini harus dilakukan secara lebih selektif dan lebih intensif lagi. Artinya peserta workshop atau pelatihan tidak boleh terlampau banyak. Untuk mengatasi keterbatasan alat, maka bila memungkinkan menggunakan fasilitas komputer milik prodi atau ruangan lain.

Lampiran-Lampiran

Lampiran 01 : Daftar Hadir Peserta



DAFTAR HADIR PESERTA PENGABDIAN MASYARAKAT PTI FIP UMJ
JUM`AT, 17 DESEMBER 2021
AUDITORIUM FIP UMJ

NO	NAMA	INSTANSI	TANDA TANGAN
1.	Robiatul Fajriah, S.Pd.I	SD Lab School FIP UMJ	
2.	Nidratun Naimi	-11-	
3.	Mega Okta Diora	SD Lab school FIP UMJ	
4.	Desy Riska Sari	SD Lab School FIP UMJ	
5.	Dewi Asih Hani. Wd	SD Lab School FIP UMJ	
6.	Tuti Haryati	SD Lab School FIP UMJ	
7.	Dwi Pangestu	SD Labschool FIP UMJ	
8.	Fuji Musiroh	SD Labschool FIP UMJ	
9.	Firyal Annabila N.S	SD Labschool FIP UMJ	
10.	Khairadha Maharani	SD Labschool FIP UMJ	
11.	Khozanah, S.Pd.I	SD Lab School FIP UMJ	
12.	Sri Mustikaningsih	SD Lab School FIP UMJ	
13.	Siti Maryam S.Pd	SD Lab School FIP UMJ	
14.	Lika Juanita	SD Lab School FIP UMJ	
15.	Reza Agwardi	SD Lab School FIP UMJ	
16.	Giriang pratama	SD Lab School FIP UMJ	
17.	Syaiful Rizal	SD Lab school FIP UMJ	
18.	Zulkifli Nasution	SD Lab school FIP UMJ	
19.	Rizky Nasution	SD Lab School FIP UMJ	
20.	Aditya prayogo.	SD Lab School FIP UMJ	

NO	NAMA	INSTANSI	TANDA TANGAN
21	Nova Dwi Santoso	SD Lab school FIP UNJ	
22	Edi prasetyo	SD LAB SCHOOL FIP-UNJ	
23.	Rizka Salamah	SD LAB SCHOOL FIP-UNJ	
24	NURUL LAILI MAFTUHAH	"	
25	ARKIANTI LALITA FATIMATUZZAHRA	"	
26	SITI NURJANAH	"	
27	DEVI WAHYUNI	"	
28	YUDA WAWANTI	"	
29	MARIYAM NOVIYANTI	"	
30	Nindi Saputri	"	
31	Firdha Syarifah	"	
32	Karimatul Ulya	SD LAB SCHOOL FIP UNJ	
33	Rizka Dwi Lestari	SD LAB SCHOOL FIP UNJ	
34	Diah Dwi Lestari	SD LAB SCHOOL FIP UNJ	
35	Lyfia Nurul Novicha	SD LAB SCHOOL FIP UNJ	
36	Fivianna Sarah	SD Lab School FIP UNJ	
37	Julia Anis Handayani	SD Lab school FIP UNJ	
38	Nurisal Jayanti	SD Lab school FIP UNJ	
39	Silvia Aprilianti S.	SD Lab school FIP UNJ	
30	Siti Rohani, S.Pd	MI Muhammadiyah	

DAFTAR HADIR PESERTA PENGABDIAN MASYARAKAT PTI FIP UMJ
JUM`AT, 17 DESEMBER 2021
AUDITORIUM FIP UMJ

NO	NAMA	INSTANSI	TANDA TANGAN
1	Zulkifli	Lab School	
2	Silvia Apriliani	— " —	
3.	Nuriah Jayanti	— " —	
4.	Fivianna Sarah	— " —	
5.	Julia Anis	— " —	
6	Zihan fauziah R.	FIP UMJ	
7.	Yoh Prastika Koto	FIP UMJ	
8.	Desy Riska Sari	Lab school	
9.	Mega Okta Diora	SD Labschool FIP UMJ	
10	M. Ishaq Gary	FIP	
11	Dr. Doly Putra	FIP	
12	Hajidah	MIS Muhamadiyah	
13.	Nursakdah	MIS Muhammadiyah	
14	Maisaroh	MIS Muhammadiyah	
15.	Didah Nuryatin	— " —	
16	Sari Suciani	MIS. Muhammadiyah	
17	Emy Farida	— " —	
18.	Sari. P	Dosen PTI	
19	Ahmad Fikri	Dosen PTI	
20	[illegible]	PTSD	

NO	NAMA	INSTANSI	TANDA TANGAN
21	Adi Kiap	Dosen PTI	
22	Yusfik Hadi	MI MI Tanjak	
23	Carnati	MI Muhammadiya	
24	Nursyamsiyah	"	
25	Fazira Adriano	FIP	

NO	NAMA	INSTANSI	TANDA TANGAN
1.			
2.	Emy Farida	MI. Muhammadiyah 01	
3.	Sari	— " —	
4.	Didah Nuryatin	— " —	
5	Maisaroh	— " —	
6	Hajidah	— " —	
7	Nursakdah	— " —	
8	Yusfik Hakim	— " —	
9	Carnati	— " —	
10	Nursyamsiyah	— " —	

Lampiran 02: Peserta yang berpartipasi mengikuti Lomba Desain Pembelajaran

Devi Wahyuni

Khairadha Maharani

Lyfia Putri

Nindi Saputri

Ukhtia Khuluqi

Robiatul Fajriah

Yuda Wawanti

Diah Dwi Lestari

Lampiran 03: Dokumentasi Kegiatan

Lampiran 04: Bukti Pengeluaran

BSI BANK SYARIAH INDONESIA

Pembayaran/Pembelian Tri Prepaid

Status: BERHASIL

Nomor Transaksi: FT22012TQHYN
Tanggal Transaksi: 12 Jan 2022 23:07:28

Nomor Struk: 20220112230718814489
Terminal: XXXXXXXX1408

PEMBELIAN: Tri Prepaid
NO HANDPHONE: 089608393108
DENOMINASI: 50000
BIAYA ADMIN: 0
NO. REF: E1CN0721007f
TOTAL DIBAYAR: Rp. 50.000

Terima kasih telah menggunakan BSI mobile.
Semoga layanan kami mendatangkan berkah bagi anda

BSI BANK SYARIAH INDONESIA

Pembayaran/Pembelian XL/Axis Prepaid

Status: BERHASIL

Nomor Transaksi: FT22012GX4H3
Tanggal Transaksi: 12 Jan 2022 23:05:48

Nomor Struk: 20220112230532336297
Terminal: XXXXXXXX1408

PEMBELIAN: XL/AXIS Prepaid
NO HP: 087872096844
DENOMINASI: 50000
BIAYA ADMIN: Rp 1,500
NO REF: 32010112096411
TOTAL DIBAYAR: Rp. 51.500

Terima kasih telah menggunakan BSI mobile.
Semoga layanan kami mendatangkan berkah bagi anda

BSI BANK SYARIAH INDONESIA

Pembayaran/Pembelian Go Pay

Status: BERHASIL

Nomor Transaksi: FT220120XYGX
Tanggal Transaksi: 12 Jan 2022 13:16:54

Nomor Struk: 20220112131627469469
Terminal: XXXXXXXX1408

PEMBAYARAN: GO PAY
NO HANDPHONE: 085711441827
NAMA CUSTOMER: GP085711441827
ADMIN FEE: 2000
NOMINAL TOP UP: 50000
NO REFF: 22011213170043335451
TOTAL DIBAYAR: Rp. 52.000

struk ini adalah bukti pembayaran yang sah

Terima kasih telah menggunakan BSI mobile.
Semoga layanan kami mendatangkan berkah bagi anda

BSI BANK SYARIAH INDONESIA

Pembayaran/Pembelian Go Pay

Status: BERHASIL

Nomor Transaksi: FT22012HSCC5
Tanggal Transaksi: 12 Jan 2022 13:07:38

Nomor Struk: 20220112130725660259
Terminal: XXXXXXXX1408

PEMBAYARAN: GO PAY
NO HANDPHONE: 085642116566
NAMA CUSTOMER: GP085642116566
ADMIN FEE: 2000
NOMINAL TOP UP: 125000
NO REFF: 22011213074442341451
TOTAL DIBAYAR: Rp. 127.000

struk ini adalah bukti pembayaran yang sah

Terima kasih telah menggunakan BSI mobile.
Semoga layanan kami mendatangkan berkah bagi anda

BSI BANK SYARIAH INDONESIA

Pembayaran/Pembelian OVO

Status: BERHASIL

Nomor Transaksi: FT22014DXJML
Tanggal Transaksi: 14 Jan 2022 13:50:54

Nomor Struk: 20220114135049106618
Terminal: XXXXXXXX1408

PEMBELIAN: OVO
NO PELANGGAN: 081214813003
NAMA PELANGGAN: TOP UP
NILAI TOPUP: 50000
ADMIN FEE: 0
TOTAL DIBAYAR: Rp. 50.000

UNTUK INFO LEBIH LANJUT :
PUSAT BANTUAN APLIKASI OVO
CS@OVO.ID /1500696

Terima kasih telah menggunakan BSI mobile.
Semoga layanan kami mendatangkan berkah bagi anda

BSI BANK SYARIAH INDONESIA

Pembayaran/Pembelian OVO

Status: BERHASIL

Nomor Transaksi: FT22012NY5G2
Tanggal Transaksi: 12 Jan 2022 13:05:42

Nomor Struk: 20220112130532324104
Terminal: XXXXXXXX1408

PEMBELIAN: OVO
NO PELANGGAN: 089609090796
NAMA PELANGGAN: TOP UP
NILAI TOPUP: 150000
ADMIN FEE: 0
TOTAL DIBAYAR: Rp. 150.000

UNTUK INFO LEBIH LANJUT :
PUSAT BANTUAN APLIKASI OVO
CS@OVO.ID /1500696

Terima kasih telah menggunakan BSI mobile.
Semoga layanan kami mendatangkan berkah bagi anda

BSI BANK SYARIAH INDONESIA

Pembayaran/Pembelian Go Pay

Status: BERHASIL

Nomor Transaksi: FT220120XYGX
Tanggal Transaksi: 12 Jan 2022 13:16:54

Nomor Struk: 20220112131627469469
Terminal: XXXXXXXX1408

PEMBAYARAN: GO PAY
NO HANDPHONE: 085711441827
NAMA CUSTOMER: GP085711441827
ADMIN FEE: 2000
NOMINAL TOP UP: 50000
NO REFF: 22011213170043335451
TOTAL DIBAYAR: Rp. 52.000

struk ini adalah bukti
pembayaran yang sah

Terima kasih telah menggunakan BSI mobile.
Semoga layanan kami mendatangkan berkah bagi anda

BSI BANK SYARIAH INDONESIA

Pembayaran/Pembelian Tri Prepaid

Status: BERHASIL

Nomor Transaksi: FT22012NMX3G
Tanggal Transaksi: 12 Jan 2022 23:06:41

Nomor Struk: 20220112230630022845
Terminal: XXXXXXXX1408

PEMBELIAN: Tri Prepaid
NO HANDPHONE: 08988580930
DENOMINASI: 50000
BIAYA ADMIN: 0
NO. REF: E1CN0620005a
TOTAL DIBAYAR: Rp. 50.000

Terima kasih telah menggunakan BSI mobile.
Semoga layanan kami mendatangkan berkah bagi anda

BSI BANK SYARIAH INDONESIA

Pembayaran/Pembelian Go Pay

Status: BERHASIL

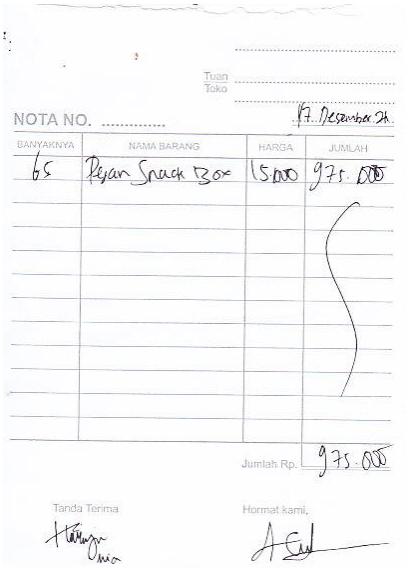
Nomor Transaksi: FT22014CN050
Tanggal Transaksi: 14 Jan 2022 13:51:57

Nomor Struk: 20220114135151933643
Terminal: XXXXXXXX1408

PEMBAYARAN: GO PAY
NO HANDPHONE: 0895333764888
NAMA CUSTOMER: GP0895333764888
ADMIN FEE: 2000
NOMINAL TOP UP: 50000
NO REFF: 22011413520329503451
TOTAL DIBAYAR: Rp. 52.000

struk ini adalah bukti pembayaran yang sah

Terima kasih telah menggunakan BSI mobile. Semoga layanan kami mendatangkan berkah bagi anda



Tuan
Toko

NOTA NO. .....

17 Desember 21

BANYAKNYA	NAMA BARANG	HARGA	JUMLAH
65	Pesan Snack Box	15.000	975.000

Jumlah Rp. 975.000

Tanda Terima

Hormat kami,

[illegible]
Tangerang Selatan
Telp. 021-7495322

ANTRIAN : 23
DRIVE THRU

8	Kombo Duo 1	363.640
3	Kombo Duo 2	136.365
5	CHARGE 1A	9.090
	Sub Total	509.095
	Dasar Pengenaan Pajak	509.095
	Pembulatan	-5
	PB1 est 10 %	50.910
	Total	560.000
	EDC MANDIRI	160.000
	Cash	400.000

Terima Kasih

[illegible]

MARTABAK KENKEN BONA

Jl. Karang Tengah Raya No. 33 Samping Plasa Bona Indah, Lebak Bulus
Jakarta Selatan
Delivery order : 0813 1899 7668 - 0857 1917 6005

MARTABAK SPECIAL	QTY			JUMLAH
	ORI	PDN		
Toblerone Keju Susu			Rp. 85.000	
Toblerone Susu			Rp. 80.000	
Ovomaltine Keju Susu			Rp. 85.000	
Ovomaltine Susu			Rp. 80.000	
Nutella Keju Susu			Rp. 85.000	
Nutella Susu			Rp. 80.000	
Komplit (Keju, Kacang, Coklat, Wijen, Susu)			Rp. 65.000	
Keju Coklat Susu			Rp. 60.000	
Keju Susu			Rp. 55.000	
Campur (Kacang, Coklat, Wijen, Susu)			Rp. 55.000	
Coklat Susu			Rp. 48.000	
MARTABAK BIASA				
Toblerone Keju Susu			Rp. 70.000	
Toblerone Susu			Rp. 65.000	
Ovomaltine Keju Susu			Rp. 70.000	
Ovomaltine Susu			Rp. 65.000	
Nutella Keju Susu			Rp. 70.000	
Nutella Susu			Rp. 65.000	
Komplit (Keju, Kacang, Coklat, Wijen, Susu)			Rp. 55.000	
Keju Coklat Susu	1		Rp. 48.000	
Keju Susu			Rp. 46.000	
Campur (Kacang, Coklat, Wijen, Susu)			Rp. 47.000	
Coklat Susu			Rp. 43.000	
TIPKER				
Toblerone Susu			Rp. 38.000	
Toblerone Keju Susu			Rp. 43.000	
Ovomaltine Susu			Rp. 38.000	
Ovomaltine Keju Susu			Rp. 43.000	
Nutalla Keju Susu			Rp. 43.000	
Nutella Susu			Rp. 38.000	
Bebas			Rp. 28.000	
MARTABAK TELOR BEBEK				
5 Telor			Rp. 60.000	
4 Telor			Rp. 58.000	
3 Telor		1	Rp. 53.000	
2 Telor			Rp. 50.000	
MARTABAK TELOR AYAM				
5 Telor			Rp. 58.000	
4 Telor			Rp. 54.000	
3 Telor			Rp. 49.000	
2 Telor			Rp. 44.000	
TOTAL				10.000

Ongkos Kirim : Jarak Dekat Rp. 2000/Antar; Jarak Jauh Rp. 5000/10.000/Antar
Nama : ....
No. Telp : ....
Alamat : ....

MARTABAK KENKEN BONA

Jl. Karang Tengah Raya No. 33 Samping Plasa Bona Indah, Lebak Bulus
Jakarta Selatan
Delivery order : 0813 1899 7668 - 0857 1917 6005

MARTABAK SPECIAL	QTY			JUMLAH
	ORI	PDN		
Toblerone Keju Susu			Rp. 85.000	
Toblerone Susu			Rp. 80.000	
Ovomaltine Keju Susu			Rp. 85.000	
Ovomaltine Susu			Rp. 80.000	
Nutella Keju Susu			Rp. 85.000	
Nutella Susu			Rp. 80.000	
Komplit (Keju, Kacang, Coklat, Wijen, Susu)			Rp. 65.000	
Keju Coklat Susu			Rp. 60.000	
Keju Susu			Rp. 55.000	
Campur (Kacang, Coklat, Wijen, Susu)			Rp. 55.000	
Coklat Susu			Rp. 48.000	
MARTABAK BIASA				
Toblerone Keju Susu			Rp. 70.000	
Toblerone Susu			Rp. 65.000	
Ovomaltine Keju Susu			Rp. 70.000	
Ovomaltine Susu			Rp. 65.000	
Nutella Keju Susu			Rp. 70.000	
Nutella Susu			Rp. 65.000	
Komplit (Keju, Kacang, Coklat, Wijen, Susu)			Rp. 55.000	
Keju Coklat Susu / Keju			Rp. 48.000	
Keju Susu			Rp. 46.000	
Campur (Kacang, Coklat, Wijen, Susu)			Rp. 47.000	
Coklat Susu			Rp. 43.000	
TIPKER				
Toblerone Susu			Rp. 38.000	
Toblerone Keju Susu			Rp. 43.000	
Ovomaltine Susu			Rp. 38.000	
Ovomaltine Keju Susu			Rp. 43.000	
Nutalla Keju Susu			Rp. 43.000	
Nutella Susu			Rp. 38.000	
Bebas			Rp. 28.000	
MARTABAK TELOR BEBEK				
5 Telor			Rp. 60.000	
4 Telor			Rp. 58.000	
3 Telor			Rp. 53.000	
2 Telor			Rp. 50.000	
MARTABAK TELOR AYAM				
5 Telor			Rp. 58.000	
4 Telor			Rp. 54.000	
3 Telor			Rp. 49.000	
2 Telor			Rp. 44.000	
TOTAL				40.000

Ongkos Kirim : Jarak Dekat Rp. 2000/Antar; Jarak Jauh Rp. 5000/10.000/Antar
Nama : ....
No. Telp : ....
Alamat : ....

Tuan ....
Toko ....

NOTA No. .... Selasa 14-12-21

BANYAKNYA	NAMA BARANG	HARGA	JUMLAH
3	Pecel Ayam Dada	16.000	96.000
3	" " Paha	"	
	+ Nasi		
		Jumlah Rp.	96.000

Tanda Terima Hormat kami,

Tuan ....
Toko ....

NOTA No. .... Selasa 14-12-21

BANYAKNYA	NAMA BARANG	HARGA	JUMLAH
6	Mie ayam pangsit	15.000	90.000
6	Mie ayam bakso	17.000	102.000
		Jumlah Rp.	192.000

Tanda Terima Hormat kami,

Indomaret

AHMAD DAHLAN RAYA 08111063676
KP. CIREUNDEU ILIR JL. IR. H. JUANDA RT 03
RW 10. 15419

14.12.21-19:19/2.1.98/FIIS 949708/AZAHR/0
1

FRUIT TEA APPLE 350	1	3500	3,500
FRUIT TEA MANGGA 350	1	3500	3,500
S-TEE BTL 330ML	1	3300	3,300
SUSU 30 TEH BOTOL 350	2	3500	7,000
ULTRA TEH KOTAK 200	1	3500	3,500
FRUIT TEA LEMON 350	1	3500	3,500
FRUIT TEA FREEZE 350	1	3500	3,500
BEAR BRAND STERIL189	1	9700	9,700

HARGA JUAL : 37,500

TOTAL : 37,500
TUNAI : 40,000
KEMBALI : 2,500

PPN : DPP= 34,091 PPN= 3,409

LAYANAN KONSUMEN SMS 0811 1500 280
CALL 1500 280 - KONTAK@INDOMARET.CO.ID

Indomaret

AHMAD DAHLAN RAYA 08111063676
KP. CIREUNDEU ILIR JL. IR. H. JUANDA RT 03
RW 10. 15419

14.12.21-12:19/2.1.98/FIIS 972908/SAHRI/0
2

ULTRA TEH KOTAK 200	17	[illegible]	59,500

HARGA JUAL : 59,500

TOTAL : 59,500
TUNAI : 110,000
KEMBALI : 50,500

PPN : DPP= 54,091 PPN= 5,409

LAYANAN KONSUMEN SMS 0811 1500 280
CALL 1500 280 - KONTAK@INDOMARET.CO.ID

Lampiran 05: Sertifikat juara lomba Desain Pembelajaran


PENDIDIKAN TEKNOLOGI INFORMASI
SERTIFIKAT
031/SERTIF/F.8-UMJ/I/2022
Diberikan Kepada
Nindi Saputri
Sebagai
"JUARA HARAPAN"
Pengabian Kepada Masyarakat
"Lomba Desain Pembelajaran"
Dekan FIP UMJ
Dr. Iswan., M.Si
Kaprodi PTI FIP UMJ
Mahbubul Wathoni, S.Si., M.Kom.


PENDIDIKAN TEKNOLOGI INFORMASI
SERTIFIKAT
031/SERTIF/F.8-UMJ/I/2022
Diberikan Kepada
Lyfia Nurul
Sebagai
"JUARA HARAPAN"
Pengabian Kepada Masyarakat
"Lomba Desain Pembelajaran"
Dekan FIP UMJ
Dr. Iswan., M.Si
Kaprodi PTI FIP UMJ
Mahbubul Wathoni, S.Si., M.Kom.


PENDIDIKAN TEKNOLOGI INFORMASI
SERTIFIKAT
031/SERTIF/F.8-UMJ/I/2022
Diberikan Kepada
Khairadha Maharani
Sebagai
"JUARA HARAPAN"
Pengabian Kepada Masyarakat
"Lomba Desain Pembelajaran"
Dekan FIP UMJ
Dr. Iswan., M.Si
Kaprodi PTI FIP UMJ
Mahbubul Wathoni, S.Si., M.Kom.


PENDIDIKAN
TEKNOLOGI
INFORMASI
SERTIFIKAT
031/SERTIF/F.8-UMJ/I/2022
Diberikan Kepada
Devi Wahyuni
Sebagai
"JUARA HARAPAN"
Pengabian Kepada Masyarakat
"Lomba Desain Pembelajaran"
Dekan FIP UMJ
Dr. Iswan., M.Si
Kaprodi PTI FIP UMJ
Mahbubul Wathoni, S.St., M.Kom.


PENDIDIKAN
TEKNOLOGI
INFORMASI
SERTIFIKAT
031/SERTIF/F.8-UMJ/I/2022
Diberikan Kepada
Robiatul Fajriah
Sebagai
"JUARA HARAPAN"
Pengabian Kepada Masyarakat
"Lomba Desain Pembelajaran"
Dekan FIP UMJ
Dr. Iswan., M.Si
Kaprodi PTI FIP UMJ
Mahbubul Wathoni, S.St., M.Kom.

Lampiran 06 : Sertifikat Narasumber Materi


PENDIDIKAN TEKNOLOGI INFORMASI

SERTIFIKAT

21a/PTI/A-05/XII/2021

Diberikan Kepada

Mahbubul Wathoni

Sebagai

"Narasumber Materi"

Pengabian Kepada Masyarakat dengan Tema Kegiatan :

"Workshop Pengaruh Desain Grafis dalam Media Pembelajaran dan Kesadaran Guru terhadap Keamanan Cyber bagi Guru, Tenaga dan Staff Pendidikan Lab School FIP UMJ"

Jakarta 20 Desember 2021

Dekan FIP UMJ

Dr. Iswan., M.Si

Kaprodi PTI FIP UMJ

Mahbubul Wathoni, S.Si., M.Kom.


PENDIDIKAN TEKNOLOGI INFORMASI

SERTIFIKAT

21a/PTI/A-05/XII/2021

Diberikan Kepada

Yasin Efendi

Sebagai

"Narasumber Materi"

Pengabian Kepada Masyarakat dengan Tema Kegiatan :

"Workshop Pengaruh Desain Grafis dalam Media Pembelajaran dan Kesadaran Guru terhadap Keamanan Cyber bagi Guru, Tenaga dan Staff Pendidikan Lab School FIP UMJ"

Jakarta 20 Desember 2021

Dekan FIP UMJ

Dr. Iswan., M.Si

Kaprodi PTI FIP UMJ

Mahbubul Wathoni, S.Si., M.Kom.


PENDIDIKAN TEKNOLOGI INFORMASI

SERTIFIKAT

21a/PTI/A-05/XII/2021

Diberikan Kepada

Ahmad Fikri Adriansyah

Sebagai

"Narasumber Materi"

Pengabian Kepada Masyarakat dengan Tema Kegiatan :

"Workshop Pengaruh Desain Grafis dalam Media Pembelajaran dan Kesadaran Guru terhadap Keamanan Cyber bagi Guru, Tenaga dan Staff Pendidikan Lab School FIP UMJ"

Jakarta 20 Desember 2021

Dekan FIP UMJ

Dr. Iswan., M.Si

Kaprodi PTI FIP UMJ

Mahbubul Wathoni, S.Si., M.Kom.


PENDIDIKAN
TEKNOLOGI
INFORMASI
SERTIFIKAT
21a/PTI/A-05/XII/2021
Diberikan Kepada
Adi Alam
Sebagai
"Narasumber Materi"
Pengabian Kepada Masyarakat dengan Tema Kegiatan :
"Workshop Pengaruh Desain Grafis dalam Media Pembelajaran dan Kesadaran Guru terhadap Keamanan Cyber bagi Guru, Tenaga dan Staff Pendidikan Lab School FIP UMJ"
Jakarta 20 Desember 2021
Dekan FIP UMJ
Dr. Iswan., M.Si
Kaprodi PTI FIP UMJ
Mahbubul Wathoni, S.Si., M.Kom.


PENDIDIKAN
TEKNOLOGI
INFORMASI
SERTIFIKAT
21a/PTI/A-05/XII/2021
Diberikan Kepada
Rikaro Ramadi
Sebagai
"Narasumber Materi"
Pengabian Kepada Masyarakat dengan Tema Kegiatan :
"Workshop Pengaruh Desain Grafis dalam Media Pembelajaran dan Kesadaran Guru terhadap Keamanan Cyber bagi Guru, Tenaga dan Staff Pendidikan Lab School FIP UMJ"
Jakarta 20 Desember 2021
Dekan FIP UMJ
Dr. Iswan., M.Si
Kaprodi PTI FIP UMJ
Mahbubul Wathoni, S.Si., M.Kom.


PENDIDIKAN
TEKNOLOGI
INFORMASI
SERTIFIKAT
21a/PTI/A-05/XII/2021
Diberikan Kepada
Sari Palestina
Sebagai
"Narasumber Materi"
Pengabian Kepada Masyarakat dengan Tema Kegiatan :
"Workshop Pengaruh Desain Grafis dalam Media Pembelajaran dan Kesadaran Guru terhadap Keamanan Cyber bagi Guru, Tenaga dan Staff Pendidikan Lab School FIP UMJ"
Jakarta 20 Desember 2021
Dekan FIP UMJ
Dr. Iswan., M.Si
Kaprodi PTI FIP UMJ
Mahbubul Wathoni, S.Si., M.Kom.

SD LABSCHOOL FIP UMJ
Jl. KH. Ahmad Dahlan Ciputat Timur Tangerang Selatan 15419 Telp./ Faks. 021 – 741 5787 www.labschoolfipumj.sch

SURAT KETERANGAN

No. 336/S.Ket/LS-SD/FIP UMJ/I/2022

Yang bertanda tangan di bawah ini, Kepala Sekolah SD Lab School FIP Universitas Muhammadiyah Jakarta menerangkan bahwa nama-nama tersebut dibawah ini :

No	Nama	NIDN/NIM	Jabatan/Golongan	Jabatan
1	Mahbubul Wathoni, S.Si., M.Kom	0307088307	Tenaga Pengajar	Ketua Prodi
2	Dr. Yasin Efendi, M.Kom.	0402117003	Lektor	Ketua Pelaksana
3	Ahmad Fikri Ardiansyah, ST, M.T.I	0309048405	Tenaga Pengajar	Anggota
4	Sari Palestina,S.Kom, M.T.I	0319018704	Tenaga Pengajar	Anggota
5	Adi Alam, S.Kom, M.SI	0311018005	Tenaga Pengajar	Anggota
6	Rikaro Rahmadi, M.Kom.	0319018704	Tenaga Pengajar	Anggota
7	Wahyu Iswantoro	2018880011	Mahasiswa	Anggota Pelaksana
8	Diah Budi Ratiningrum	2018880010	Mahasiswa	Anggota Pelaksana
9	Mia Hariyani	2018880008	Mahasiswa	Anggota Pelaksana
10	Delina Syarfina	2018880006	Mahasiswa	Anggota Pelaksana
11	Yoli Prastika Koto	2018880007	Mahasiswa	Anggota Pelaksana
12	Zihan Fauziah Rahmah	2019880008	Mahasiswa	Anggota Pelaksana
13	Salsa Syahla Habibah	2019880006	Mahasiswa	Anggota Pelaksana
14	Ratna Ayu Setyawati	2019880012	Mahasiswa	Anggota Pelaksana
15	Azriel Putra Junaedi	2019880009	Mahasiswa	Anggota Pelaksana

Telah melaksanakan kegiatan Pengabdian Masyarakat sebagai Pembicara atau narasumber dan panitia pelaksana kegiatan Worshop bagi para guru, tenaga dan staff pendidikan di Sekolah Dasar (SD) Lab Scholl FIP Universitas Muhammadiyah Jakarta (UMJ) yang dilaksanakan pada hari Jum' at tanggal 17 Desember 2021 dengan materi sebagai berikut :

1. Pengaruh Desain Grafis dalam Media Pembelajaran, mulai pukul 8.00 s.d 11.30
2. Kesadaran Guru terhadap Keamanan Cyber, mulai pukul 13.30 s.d 17.00

Demikian surat keterangan ini dibuat untuk dapat dipergunakan sebagaimana mestinya.
Atas perhatian dan kerjasama kami ucapkan terima kasih.

Tangerang Selatan , 20 Desember 2021
a.n. Kepala Sekolah
Wakasek Kesiswaan

Siti Nurjanah, S.Sos

SD LABSCHOOL FIP UMJ
Jl. KH. Ahmad Dahlan Ciputat Timur Tangerang Selatan 15419 Telp./ Faks. 021 – 741 5787 www.labschoolfipumj.sch

Tangerang Selatan, 20 Desember 2021

Nomor : 337/S.Ket/LS-SD/FIP UMJ/I/2022
Lamp : -
Perihal : **Ucapan Terimakasih**

Kepada
Yth **: Ketua Prodi Pendidikan Teknologi Informasi**
Fakultas Ilmu Pendidikan, Universitas Muhammadiyah Jakarta
Di -
Tempat

Assalamu'alaikum Warahmatullahi Wabarakatuh

Sehubungan dengan telah selesainya kegiatan Pengabdian Masyarakat dengan materi workshop

1. Pengaruh Desain Grafis dalam Media Pembelajaran
2. Keasadaran Guru terhadap Keamanan Cyber

Adapun waktu pelaksanaan dilaksanakan selama 1 (satu) hari yakni hari Jumat, 17 Desember 2021 mulai pukul 8.00 s.d 17.00 WIB.

Kami mewakili guru, tenaga dan staff SD Lab School FIP UMJ mengucapkan terimakasih kepada Ketua Prodi Pendidikan Teknologi Informasi, Fakultas Ilmu Pendidikan, Universitas Muhammadiyah Jakarta, yang telah menugaskan staff dosen dan mahasiswanya untuk memberikan Workshop atau pelatihan *bagi* guru, tenaga dan staff pendidikan SD Lab School FIP UMJ.

Demikian Surat ini kami sampaikan, semoga kedepan terjalin kerjasama yang lebih baik lagi. Atas perhatian dan kerjasamanya kami ucapkan terima kasih.

Wassalamu'alaikum Warahmatullahi Wabarakatuh

a.n Kepala Sekolah
Wakasek Kesiswaan

Siti Nurjanah, S.Sos