



NEWS LETTER



April, 2020



CTCT & IT, Ranchi, Jharkhand



Shri Amit Taneja, DIGP
Patron

Shri Rajesh Sahay, Comdt.
Chief Editor

Shri Sanjay Belwal, DC.
Editor & Publisher

Index

Topic	Author	Page No
1. How Scientists Captured the First Image of a Black Hole	SI/DM K S Gharade	3
2. Mesh Radio Networking	ASI/T Nagabushan	5
3. Why Is Digital Security So Important?	ASI/C Vishnu Kumar	8
4. Brain-Computer Interface	HC/RO Anuj Kumar	10
5. Quiz	R & D Team	11
6. Technical Terms	R & D Team	13
7. Answers To Quiz	R & D Team	14

“Technology is best when it brings people together.”

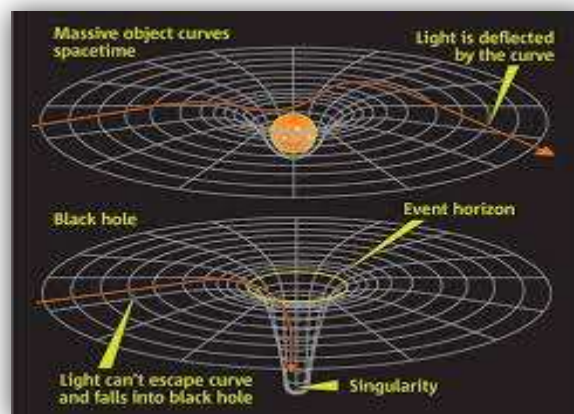
How Scientists Captured the First Image of a Black Hole

SI/DM K S Gharade

What is a Black Hole?

A black hole is a region of spacetime where gravity is so strong that nothing—no particles or even electromagnetic radiation such as light—cannot escape from it. The theory of general relativity predicts that a sufficiently compact mass can deform spacetime to form a black hole. The boundary of the region from which no escape is possible is called the event horizon. Although the event horizon has an enormous effect on the fate and circumstances of an object crossing it, it has no locally detectable features. In many ways, a black hole acts like an ideal black body, as it reflects no light. Moreover, quantum field theory in curved spacetime predicts that event horizons emit Hawking radiation, with the same spectrum as a black body of a temperature inversely proportional to its mass. This temperature is on the order of billionths of a kelvin for black holes of stellar mass, making it essentially impossible to observe.

Objects whose gravitational fields are too strong for light to escape were first considered in the 18th century by John Michell and Pierre-Simon Laplace. The first modern solution of general relativity that would characterize a black hole was found by Karl Schwarzschild in 1916, although its interpretation as a region of space from which nothing can escape was first published by David Finkelstein in 1958. Black holes were long considered a mathematical curiosity; it was not until the 1960s that theoretical work showed they were a generic prediction of general relativity. The discovery of neutron stars by Jocelyn Bell Burnell in 1967 sparked interest in gravitationally collapsed compact objects as a possible astrophysical reality.

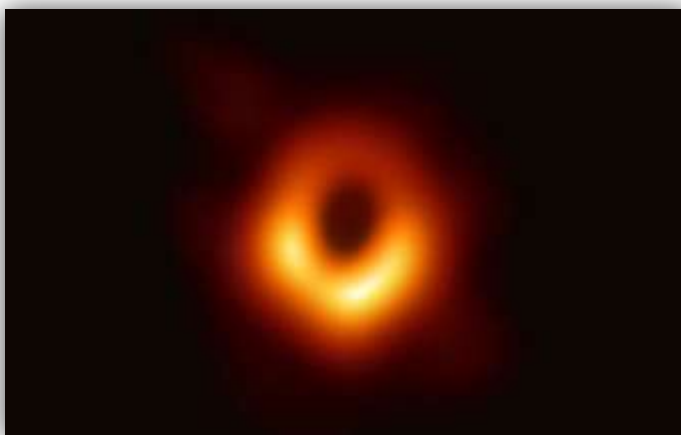


In the News

Accomplishing what was previously thought to be impossible, a team of international astronomers has captured **an image of a black hole's silhouette**. Evidence of the existence of black holes – mysterious places in space where nothing, not even light, can escape – has existed for quite some time, and astronomers have long observed the effects on the surroundings of these phenomena. In the popular imagination, it was thought that capturing an image of a black hole was impossible because an image of something from which no light can escape would appear completely black. For scientists, the challenge was how, from thousands or even millions of light-years away, to capture an image of the hot, glowing gas falling into a black hole. An ambitious team of international astronomers and computer scientists has managed to accomplish both. Working for well over a decade to achieve the feat, the team improved upon an existing radio astronomy technique for high-resolution imaging and used it to detect the silhouette of a black hole – outlined by the glowing gas that surrounds its event horizon, the precipice beyond which light cannot escape. Learning about these mysterious structures can help students understand gravity and the dynamic nature of our universe, all while sharpening their math skills.

How They Did It

Though scientists had theorized they could image black holes by capturing their silhouettes against their glowing surroundings, the ability to image an object so distant still eluded them. A team formed to take on the challenge, creating a network of telescopes known as the Event Horizon Telescope, or the EHT. They set out to capture an image of a black hole by improving upon a technique that allows for the imaging of far-away objects, known as Very Long Baseline Interferometry, or VLBI.



Telescopes of all types are used to see distant objects. The larger the diameter, or aperture, of the telescope, the greater its ability to gather more light and the higher its resolution (or ability to image fine details). To see details in objects that are far away and appear small and dim from Earth, we need to gather as much light as possible with very high resolution, so we need to use a telescope with a large aperture.

That's why the VLBI technique was essential to capturing the black hole image. VLBI works by creating an array of smaller telescopes that can be synchronized to focus on the same object at the same time and act as a giant virtual telescope. In some cases, the smaller telescopes are also an array of multiple telescopes. This technique has been used to track spacecraft and to image distant cosmic radio sources, such as quasars.

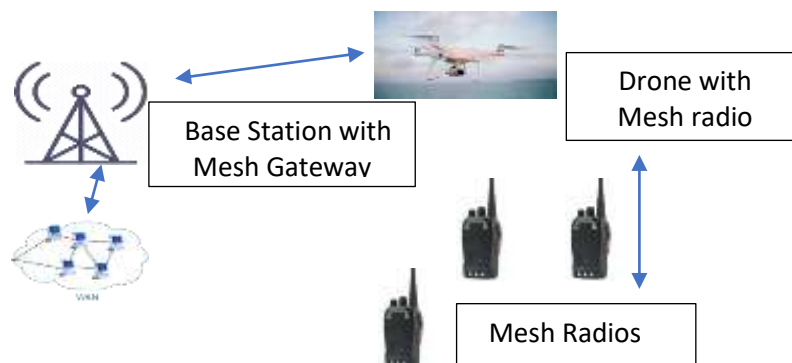
(Scientists have obtained the first image of a black hole, using Event Horizon Telescope observations of the centre of the galaxy M87. The image shows a bright ring formed as light bends in the intense gravity around a black hole that is 6.5 billion times more massive than the Sun. Image credit: Event Horizon Telescope Collaboration)

Mesh Radio Networking

ASI/T Nagabushan

What is Mesh Radio Networking?

Mesh Radio networks are the newest innovation in wireless technology. Historically, all wireless networks suffered from the same limitations imposed on wired networks. The information path was limited to one single route back to a central data point. If that one route was unavailable, then the entire network was unusable. The network was entirely dependent upon every node on the network being active at all times. Given the vagaries of weather, technical problems, user error, or malfunctioning equipment, maintaining a single route wireless network was very difficult. Users of single route wireless networks found them complex to install, very difficult to maintain, subject to low transmission rates with unacceptable performance levels.



Introduction

Wireless mesh network is a network which comprises various wireless nodes with access points. Each node in the network acts as a forwarding node to transfer the data. Since the network is decentralized, forwarding of data is possible only to the neighbouring node. This results in the network structure simple and easy. WMN makes the people connected with the Internet who work at remote areas and operating business. This chapter throws light on WMN architecture, layer functionalities, various other networking standards, and applications.

Wireless mesh network

Architecture Wireless mesh network is the architecture which provides less mobility with low cost within a radio range. WMN is an infrastructure which is a network of routers minus cabling between the nodes. It consists of radio nodes which need not to be cabled to a wired port like the conventional wireless access points. Shortest hops are predicted to transmit the data toward large distance. Nodes between the source and destination act as a forwarding node which works cooperatively in making decisions in route prediction based on the topology and forwarding the data.

Wireless mesh network provides stability when compared to the rest of the network topologies rather than the node addition or deletion in the network. In infrastructure mesh network, the data forwarding and receiving are via gateway, whereas in the rest of the network, it is through pair of nodes. The frequency of link breakage is higher in the case of wireless mesh networks when there is a high mobility which results in low performance in communication of information.

Wireless mesh networks are categorized into three types based on the functionality of the nodes in the network:

- Infrastructure mesh architecture
- Mesh architecture based on clients
- Hybrid mesh architecture

Infrastructure mesh architecture

Mesh routers together act as a wireless back bone for infrastructure mesh architecture. Client node is passive in mesh infrastructure via Ethernet links; conventional clients with Ethernet interfaces can be connected to mesh routers. If the traditional network and the mesh router are operating under the same radio range, then it is easy for the mesh network to communicate with the mesh router. Alternatively, if the radio ranges differ, the nodes will communicate to the base station so that with the help of Ethernet, it can be further communicated to the mesh routers.

Mesh architecture based on client is the one in which the client nodes are connected from peer to peer. Each node can act as a routing node to transfer the data. Here, the client performs the role of mesh routing by acting in the forwarding of the data packets.

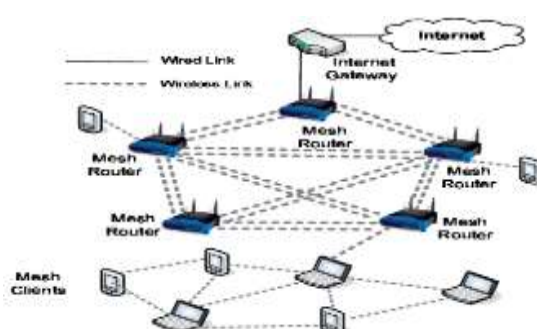
Hybrid mesh architecture In hybrid mesh architecture, usually the mesh nodes/router acts as a back bone of the entire network operation. With the help of network mesh router, it performs routing and forwarding of data packets toward its destination

Characteristics of wireless mesh networks

- **Dynamic self-configuration and self-organization**
- **Adaptation**
- **Fault tolerance and robustness**
- **Low-cost**
- **Integration and interoperability**

Management

The infrastructure-based wireless mesh network is a decentralized network without a centralized management or with no centralized server which is more expensive. These methods are more reliable and efficient as each node has to transmit to the next node. Here, nodes act as router to transmit the data to its peers which are located far even it is a single hop. Wireless mesh network should be stable, i.e., there should not be high mobility. If node failure occurs due to any hardware problem or any other, the neighbour node will perform rerouting with the help of routing protocols.



PR9560 Advanced VHF COMSEC/ECCM radio systems

Advanced VHF COMSEC/ECCM radio systems for reliable voice and data communications

The PR9560 is intended for land forces such as infantries, forward observers, snipers, special forces and antiterror units, and can be deployed at the platoon or company level. The radio owns compact, lightweight and ruggedized characters, which assures reliability and maneuverability in demanding mission critical conditions.



The PR9560 provides continuous coverage in the 30~87.975 MHz frequency band. By applying with the Software Defined Radio (SDR) architecture, the radio offers three progressive waveforms (CNR/VRN/PRN) to guarantee a more stable transmission, longer distance and greater speed for secured communication. With the high data throughput, it benefits to weapon system control, battlefield supervision and real-time situational awareness.

The Tianhai VHF handheld radio is packed with numerous advanced functionalities, for instance: simultaneous voice and data, automatic position reporting using an internal or external GPS receiver, VOX, integration with tactical messaging or image transmission applications.

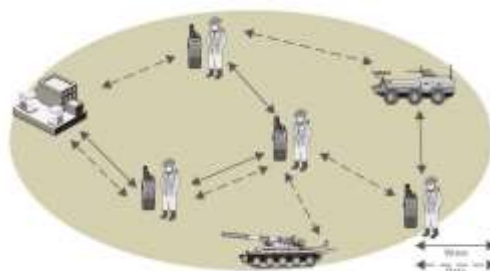
ADVANCED WAVEFORMS Combat Net Radio (CNR)

CNR's primary role is voice or data transmission in battlefield via point to point/ point to multi-points communication. The CNR attributes 4 modes: FM (Frequency Modulation), FF (Fixed Frequency), FH (Frequency Hopping) and FCS (Free Channel Search)



Voice Relay Network (VRN)

VRN extends voice communication distance by chaining, resolves the communication issues in complicated scenarios, for example underground, jungle and trench. The VRN can be spread up to 6 hops relaying in both FF and FH modes.



Packet Radio Network (PRN)

PRN mainly serves as data transmission for man to machine and machine to machine in battlefield. Based on Mobile Ad-Hoc Network (MANET) technology, the PRN contains abilities of decentralization, self-healing, self-forming, dynamic topology and simultaneous voice and data. The transmission distance can be stretched significantly by up to 6 hops in 32 nodes maximum.

HIGHLIGHTS : Electronic Counter-Counter Measures(ECCM)

Frequency Hopping (FH) : The radio contains a frequency hopping rate of 1,000 hops per second which ensures the communication can be succeeded with up to 70 % of working band interfered, whereas the communication distance will not be degraded

Free Channel Search (FCS) :FCS mode is intended for operations that requires frequency agility in an high-noise or wideband radio jamming environment.

Communication Security (COMSEC)

Encryption : The PR9560 provides AES 256 bit software encryption for both voice and data communication, as well as supports customized encryption board.

Key filling: Key fill gun offers 6 functions: confidential information storage, networking configurations injection, encryption parameters backup, identity authentication, key erasing execution and also reserves key storage ability even if in the event of power loss.

Key erasing: The radio affords diverse methods to prevent the secured information disclosure through erasing the key manually or automatically, i.e., manually erasing the key by holding the combined buttons even if the radio is shut down; automatically erasing the key when the radio was disassembled.

Reliability : Optimized Battery Performances

Continuously working for at least 12 hours (1:1:8,3,800mAh) through the unique adaptive energy saving technique. The operation temperature can be expanded to -40°C ~ +65°C by adopting the low temperature battery.

Ruggedized :The PR9560 and its accessories are certified MIL-STD-810G, with a improved waterproof capability of submersion in 2 meters water for up to 4 hours.

Usability: Small-profile (220H×72.5W×36.5D) and lightweight (<600g) design guarantees portable capability in the front-line.

GPS build-in module enables Team Leaders at the tactical level to track individual soldier position location information (PLI), enabling situational awareness.

OLED screen provides high brightness, wider viewing range, and readable capability under direct sunlight.

Power and volume buttons are separated along both sides of PTT button to prevent mistakenly touch.

Versatile applications such as data transmission software, PC programming kit and dispatch platform offer immediate manipulation readiness.

Why Is Digital Security So Important?

ASI/C Vishnu

Whether it is through growing use of smartphones, social media, e-commerce or other means, we are all putting our personal information on internet more and more. We are living in a time of unprecedented connectivity, and it is easy to forget that there are dangers out there, on the internet, on social media, in the apps we use every day.

Even worse, you may have used the same password on other accounts (banking, email, government sites), which means the person who got your Facebook password might be able to access those accounts too. And if someone gets into your email account, they could change your password at virtually every website by sending a reset link to that email address. When any aspect of your digital security is relaxed, all of your personal information - your credit cards, bank accounts, email accounts, ***your whole identity*** could be at risk.

Things That Make You more Vulnerable are :

Weak Passwords

One way a hacker can obtain your passwords is by simply trying multiple times on one site. They would simply log in, again and again. This works if the password is common, e.g. "password" or "password1". Generally these attacks fail, but do work a certain percentage of the time on accounts with a poor password.

Sharing passwords

From time to time it might be convenient to share a password to one of your accounts with someone else. This could lead to your password(s) unintentionally (or intentionally) ending up in the wrong hands. Also, that person might start using your password with their own accounts. If their password gets discovered by bad guys, it could end up on the "common passwords" list they use to crack accounts, leaving you vulnerable.

Using the same password for each website

With all the websites we visit each day, each with their own password requirements (include a capital, lower case, number, special character, etc.), it can be very tempting to create one password that meets all of those requirements and then use that same password for every site.

While this makes it a lot easier for you to remember your password for each website, it also makes it a lot easier for a hacker to gain access to each of your accounts. Let's say your favourite social media site got hacked and your password was stolen. Now those hackers have the password to all of your accounts on every website. Scary thought.

Writing Your Passwords Down

Writing your passwords down, on paper or in a file/email, leaves you vulnerable. If someone finds that paper, or you lose your notebook, your accounts could be at risk. If you keep a list of your passwords in a Word doc or an email, you could be vulnerable too. If someone accesses your computer, they could find easily that list. If you don't think you can remember all your passwords without writing them down, you should use a password manager program.

Password Reset Options and Compromised Email Accounts

Most websites offer a "forgot password" option where a password reset link is emailed to the email address listed on your account. This is a great, secure way to get into your account should you forget your password.

Where it becomes a vulnerability is if an attacker gets access to the email account listed for password resets. The attacker could reset your passwords to every online account you have, have access to those accounts, and you'd be locked out.

A good way to insulate yourself is to have a second email address which you use as the password reset email address for your most important accounts (banking, government, etc.). Use your primary email for social media and e-commerce (which are easier targets for hackers), but use your 2nd secure address for banking and government sites only.

How to Make Passwords & Keep Them Secure

Make your Passwords Impossible to Guess A strong password generally should include these common features:

- Lower Case
- Upper Case
- Numbers
- Special Characters
- 10+ Characters

Make sure to include all of these in your passwords. Make your password as long as possible, but not so long that you can't remember it. A great way to make a super-secure password that you can easily remember is to think of it as a *passphrase* instead of a *password*.

For example: **A8dA@6dk*^DAfsdfd#a097**. This would be a very secure password. It's long, has upper case, lower case, numbers and special characters. Problem is nobody would ever be able to remember it!

DragonsAre110%Magical

Now *that* is easy to remember! Look, you've already memorized it! (But don't use it, or any example, as your password!) Or you can string a few nonsensical words together, separated by special characters and numbers. 21^Blue^Lemons^Tiger.

No Two Passwords Should Be the Same

Ensure each password you use on your accounts is unique. *No two passwords should be the same*. Don't use variations of the same root password either.

For example: Don't make the password for one system "IloveCorvettes" and the password for another system "IloveCorvettes1".

Don't reuse passwords across multiple sites. Reusing passwords for email, banking, and social media accounts can lead to identity theft.

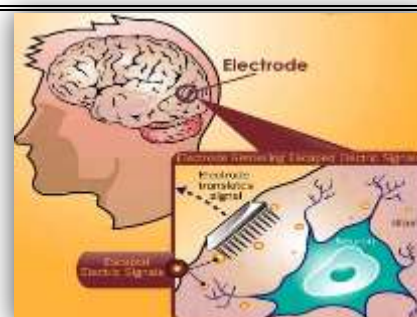
Key points to remember when setting up your home Wi-Fi network:

- ✓ Enable encryption on your access point (router/gateway)
- ✓ Do not use WEP encryption
- ✓ Use WPA or WPA2 encryption
- ✓ Select a long, secure password (use the same methodology you have learned about in this course to make the password)
- ✓ Change your Wi-Fi network name (SSID) from the default name to something unique. Default SSIDs are very obvious, and to hackers indicate a "soft target" (a network setup by a novice, meaning it is likely easier for them to hack).
- ✓ Don't disable the SSID Broadcast option
- ✓ Disable remote login
- ✓ Disable wireless administration (meaning you'll need to plug directly into the router to change any settings)

Brain-Computer Interface

HC/RO Anuj Kumar

Technology has made it possible to make use of computers as a replacement for the brain. Many kinds of research are going on to reduce the human work. The world is marching towards the automation in order to reduce the complexity in the work, speed up the process and at the same time to provide a relaxed life to all mankind. Some of the technologies involving human brain are the blue brain project, the blue eyes technology.



What is a Brain-Computer Interface?

Brain-computer interface (BCI) is a collaboration between a brain and a device that enables signals from the brain to direct some external activity, such as control of a cursor or a prosthetic limb the interface enables the direct communications pathway between the brain and object to be controlled.

The human brain is of the size of a deflated volleyball which weighs about 3 pounds. We live at a time when the disabled are on the leading edge of a border societal trend towards the use of an assistive technology known as Brain with Computer Interface. With the advent of miniature wireless tech, electronic gadgets have stepped up the invasion of the body through innovative techniques.

Introduction:-

A Brain-computer interface (BCI) provides a new communication channel between the human brain and the computer. The 100 billion neurons communicate via minute electrochemical impulses, shifting patterns sparking like fireflies on a summer evening, which produce movement, expression, and words. Mental activity leads to changes of electrophysiological signals. The BCI system detects such changes and transforms it into a control signal. In the case of cursor control, for example, the signal is transmitted directly from the brain to the mechanism directing the cursor, rather than taking the normal route through the body's neuromuscular system from the brain to the finger on a mouse. By reading signals from an array of neurons and using computer chips and programs to translate the signals into action, BCI can enable a person suffering from paralysis to write a book or control a motorized wheelchair or prosthetic link through thought alone. Many physiological disorders or injuries such as high-level spinal cord injury can disrupt the communication path between the brain and the body. This is where brain-computer interface comes into play contributing for beneficial real-time services and applications.

How does the brain-computer interface work? Brain Computer Interface:-

Our brains are filled with neurons, individual nerve cells connected to one another by dendrites and axons. Every time we think, move, feel or remember something, our neurons are at work. That work is carried out by small electric signals that zip from neuron to neuron as fast as 250 mph. The signals are generated by differences in electric potential carried by ions on the membrane of each neuron. Although the paths the signals take are insulated by something called myelin, some of the electric signal escapes. Scientists can detect those signals, interpret what they mean and use them to direct a device of some kind. It can also work the other way around. For example, researchers could figure out what signals are sent to the brain by the optic nerve when someone sees the color red. They could rig a camera that would send those exact signals into someone's brain whenever the camera saw red, allowing a blind person to "see" without eyes.

Technical Quiz

R&D Team

-
1. **Robot is derived from Czech word**

(A) Rabota
(B) Robota
(C) Rebota
(D) Ribota

 2. **The main objective(s) of Industrial robot is to**

(A) To minimise the labour requirement
(B) To increase productivity
(C) To enhance the life of production machines
(D) All of the above

 3. **Drives are also known as**

(A) Actuators
(B) Controller
(C) Sensors
(D) Manipulator

 4. **Why would a hacker use a proxy server?**

(A) To create a stronger connection with the target.
(B) To create a ghost server on the network.
(C) To obtain a remote access connection.
(D) To hide malicious activity on the network.

 5. **What type of symmetric key algorithm using a streaming cipher to encrypt information?**

(A) RC4
(B) Blowfish
(C) SHA
(D) MD5
-

6. **To hide information inside a picture, what technology is used?**
- (A) Rootkits
 - (B) Bitmapping
 - (C) Steganography
 - (D) Image Rendering
6. **Which phase of hacking performs actual attack on a network or system?**
- (A) Reconnaissance
 - (B) Maintaining Access
 - (C) Scanning
 - (D) Gaining Access
7. **Attempting to gain access to a network using an employee's credentials is called the _____ mode of ethical hacking.**
- (A) Local networking
 - (B) Social engineering
 - (C) Physical entry
 - (D) Remote networking
8. **What type of rootkit will patch, hook, or replace the version of system call in order to hide information?**
- (A) Library level rootkits
 - (B) Kernel level rootkits
 - (C) System level rootkits
 - (D) Application level rootkits
9. **What is the purpose of a Denial of Service attack?**
- (A) Exploit a weakness in the TCP/IP stack
 - (B) To execute a Trojan on a system
 - (C) To overload a system so it is no longer operational
 - (D) To shutdown services by turning them off

Technical Terms

R&D Team

SDK (SOFTWARE DEVELOPMENT KIT)

SDK is a set of tools for creating specific types of software. SDK's are released by companies that control the platform the software is being developed for. For instance, apps developed for iOS require the iOS SDK, Windows apps require the .NET Framework SDK, and Java apps require the Java Development Kit.

HYBRID APP

Hybrid apps are applications that will work on different platforms (computers, mobile devices, tablets) and are a combination of a native app (one that is stored locally on your device) and a web app (one that is accessed through a web browser on the Internet). Amazon and Apple App Stores, Twitter, Yelp, and Gmail are all examples of hybrid apps.

DATA VISUALIZATION

Data visualization is the use of graphs, charts, tables, infographics, etc. in order to define and communicate data being analysed and the findings that have come from it.

BIG DATA

Big data is a term for collections of data that are so large they can't be processed through traditional data processing systems. These collections come from sources like mobile devices, emails, search keywords, user database information, applications, and servers. By finding ways to comb through this data, companies can identify consumer patterns and use them to predict and optimize their business.

MOOD BOARD

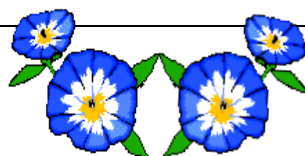
Mood boards are collections of content (images, materials, pieces of text) used to represent the visual style of a website—or any creative project— (colour palette, images, icons, and fonts) in pre-production. The style represented on a mood board is then translated into digital form by visual designers.

A/B TESTING

A/B testing is the practice of comparing two versions of online content—websites, apps, marketing emails, etc.—in order to see which version performs better. The two versions (A and B) are presented to users at random in order to gauge reactions.

Acknowledgement

We are highly thankful for reading out this compilation and hope it will be useful for you in our day to day professional and personal life. We would like to hear your interest areas, suggestions from you to make this newsletter more informative and interesting. Your views will definitely help us to create this newsletter as an effective medium to reach you with latest development in the fields of communication and technology.



R&D Team

CTC T&IT CRPF, Ranchi, Jharkhand

✉ ctcit@crpf.gov.in

Answers to the Quiz

1	2	3	4	5	6	7	8	9	10
B	D	A	D	A	C	D	A	A	C