2020-21 | ISSUE 2

ASCII NEWSLETTER

ASSOCIATION OF STUDENTS OF COMPUTER SCIENCE FOR INFORMATION INTERCHANGE

WHAT'S INSIDE THIS ISSUE

RESEARCH ON CYBERSECURITY

SNOWDEN

INTERESTING FACTS

STUDENTS CORNER

INTERNET SAFETY WHILE BROWSING

SUCCESSFUL PEOPLE - CYBERSECURITY

Welcome!

The ASCII Club is launching the second issue of the academic year 2k20-21.

We the students of ASCII, welcome you all to the interesting field of cyber-security!!

It's filled with interesting facts, art, and an achievements section at the end!

Department of Computer Science and Engineering

Vision:

To be acclaimed internationally for excellence in teaching and research in Computer Science & Engineering, and in fostering a culture of creativity and innovation to responsibly harness state-of-the-art technologies for societal needs.

Mission:

Mission 1: To assist students in developing a strong foundation in Computer Science and Engineering by providing analytical, computational thinking and problem solving skills.
Mission 2: To inculcate entrepreneurial skills to develop solutions and products for interdisciplinary problems by cultivating curiosity, team spirit and spirit of innovation.
Mission 3: To provide opportunities for students to acquire knowledge of state-of-the-art in Computer Science and Engineering through industry internships, collaborative projects, and global exchange programmes with Institutions of international repute.
Mission 4: To develop life-long learning, ethics, moral values and spirit of service so as to contribute to the society through technology.
Mission 5: To be a premier research-intensive department by providing a stimulating environment for knowledge discovery and creation.

B.Tech Programme Educational Objectives (PEOs)

The Computer Science & Engineering Program graduates will
PEO1: Strive on a global platform to pursue their professional career in Computer Science and Engineering.
PEO2: Contribute to product development as entrepreneurs in inter disciplinary fields of engineering and technology.
PEO3: Demonstrate high regard for professionalism, integrity and respect values in diverse culture, and have a concern for society and environment.

B.Tech Programme Outcomes (PO's) and Programme Specific Outcomes (PSO's)

PO1: Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
PO2: Problem analysis: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
PO3: Design and development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
PO4: Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
PO5: Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.
PO6: The engineer and society: Apply reasoning informed by the contextual knowledge to Assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
PO7: Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of and need for sustainable development.
PO8: Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
PO9: Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
PO10: Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
PO11: Project management and finance: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
PO12: Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.
PSO1: Adopt Standard Practices: Ability to design and engineer, innovative, optimal and elegant computing solutions to interdisciplinary problems using standard practices, tools and technologies.
PSO2: Research and Innovation: Ability to learn emerging computing paradigms for research and innovation

CYBER SECURITY

BY VEDHA

In the 21st century, every piece of information about us and the world is gathered and stored in digital form in programmed machines. There are lots of ways to misuse this information. In the digital world we have data defenders who guard the data from black hat hackers. They do so through a general platform called cyber security. But, what is cyber security? Cyber security is a system which protects our network, devices, programs and data from attacks, damages and unauthorized access through the use of tools and technology.

The Original Logic Bomb

Most prominent cyber - attacking missions are done by the USA. This cyber attack was also carried out by the USA on Russia. This particular attack happened in 1982 but there was persistent rivalry between these two countries for a long time. This cold war came to international notice when these two countries fought for crude oil in Antarctica. But before this cold war this cyber attack is the only notable debate between these two countries. President Ronald Wilson Reagan took charge of this attack.

With his permission, the CIA destroyed a Siberian oil pipeline of Russia without using traditional explosives like missiles.

References : https://www.inuth.com/

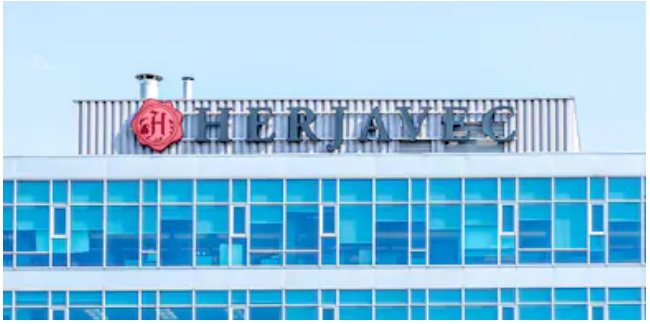
Herjavec Group

BY MAHIMA

Organizations should build their security programs, understanding that no matter how many firewalls or network controls they have in place, the risk of insider threats will always be present. In light of the ever-evolving threat landscape, increased inter-connectivity that is being driven by the rising popularity of Internet-of-Things (IoT), and rising remote work scenarios, one thing is clear – the strength of an organization's cyber hygiene relies on the internal security practices implemented. To help us out, we have, the Herjavec Group - CYBERSECURITY is what they do and they're good at it. Herjavec Group is the top-ranked trusted MSSP(Managed Security Services Provider) in the world.

Their history started in 2003 when IT entrepreneur Robert Herjavec founded Herjavec Group to provide security products and services to enterprise organizations. They provide security services, advisory services, managed security services, identity services, PCI compliance, Security Operations, Threat Detection, Security Technology Engineering, Advisory Services, Identity Services, Technology Implementation, Threat Management, and Incident Response.

They have offices and Security Operations Centers across the United States, the United Kingdom, and Canada. As of today, the Herjavec group is worth over $200 million.



Herjavec Group is a top-certified partner with partnerships with many of the industry's leading technology providers, some of which include being a Palo Alto Networks Diamond Level Partner, Splunk Global Service Alliance Partner and Professional Services Partner, and McAfee MASP Support Provider and Platinum Partner. An interesting fact to be noted is that each member of the firm is given one full day every year to volunteer their services in their local communities. They also offer employment opportunities for those who are interested in contributing their skills in the field of cybersecurity. On October 29,2019, the Herjavec Group Executive Leaders held a live, interactive Q&A webinar to wrap-up Cybersecurity Awareness Month. On February 5, JR Cunningham, VP of Strategic Solutions at Herjavec Group, hosted a webinar on how organizations can secure their digital transformation directives in 2020.

References:

https://www.herjavecgroup.com

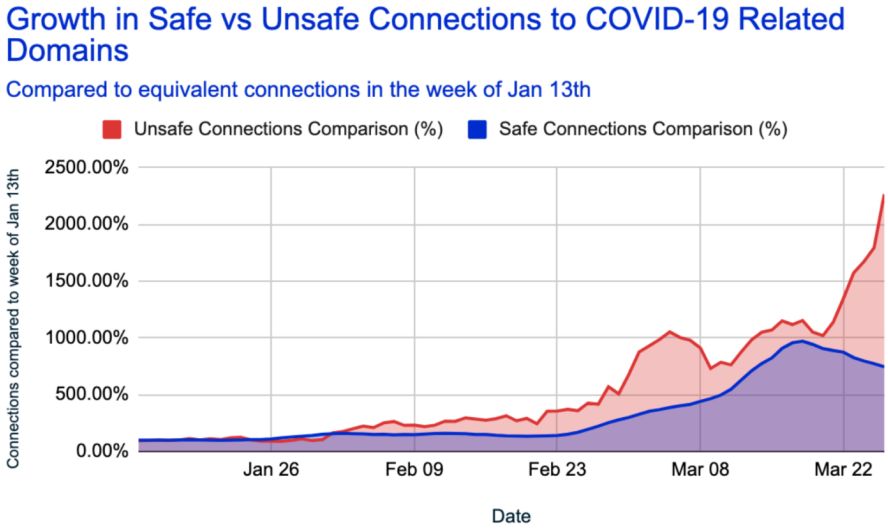
RESEARCH ON CYBER SECURITY: ANALYSIS: INTERNET TRAFFIC RELATED TO CORONAVIRUS-THE GOOD AND THE BAD

BY SNEHA

Published on :April 12, 2020

The experts analyzed year-to-date queries from around the globe that were related to COVID-19. This analysis included visits to official sites that provide information on the virus, such as the WHO and CDC, as well as prominent healthcare institutions and newly registered domains that utilize keywords associated with the novel coronavirus.

Analyzing growth rates of traffic to good and bad sites



The two plotted trend lines on the same graph show how the growth rates of traffic to both safe and malicious sites across the 3-month period.

It was found that the number of visits to known-bad sites was 22 times higher at the end of March than it was at the beginning of the year. Comparatively, the number of visits to safe sites has only increased 6.5 times in the same period of time. This indicates that the volume of traffic to bad sites is currently growing much faster than traffic to safe sites.

Based on the trends we see here, we expect the volume of traffic to known-bad COVID-19 related sites will continue climbing as bad actors tap into new waves of interest in various news angles.

References: https://www.zdnet.com

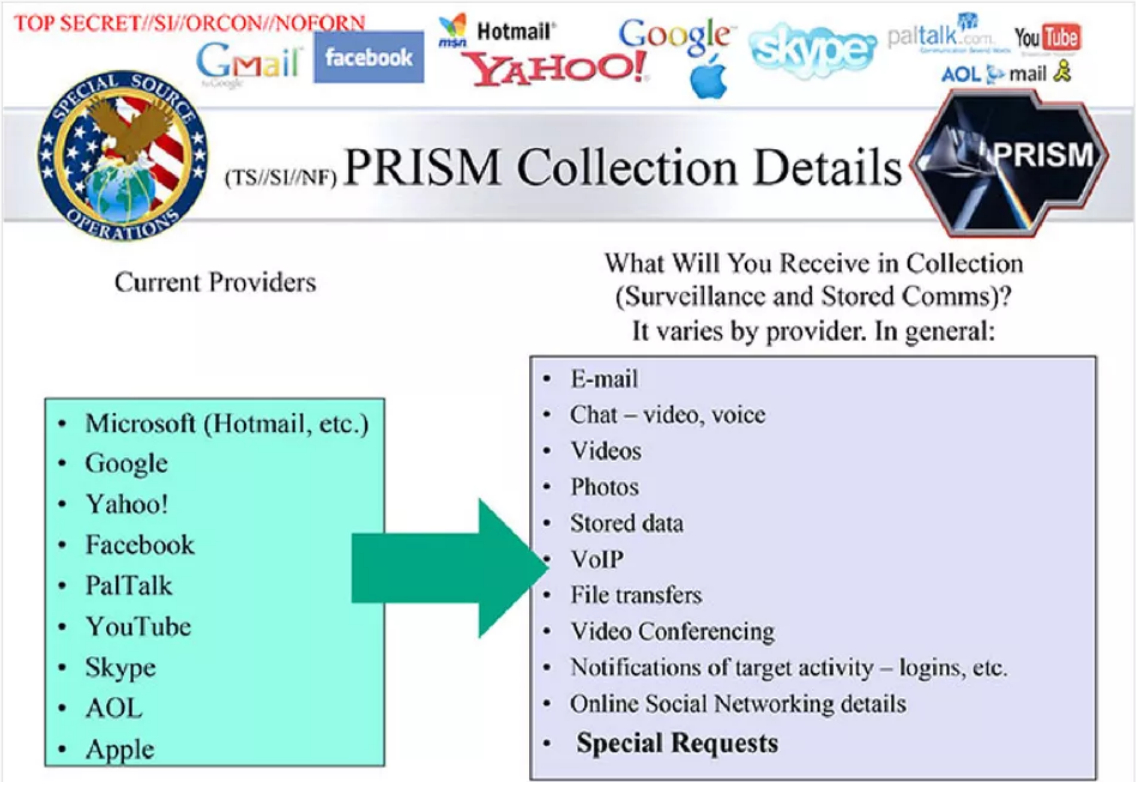
SNOWDEN AND CYBERSECURITY

BY SANGEERTHANA

"We have moved to a society in which we are forced to live our lives naked before power".

-EDWARD JOSEPH SNOWDEN

Edward Snowden, the ex CIA employee turned whistle-blower, brought to light the PRISM operation through which the NSA secured access to the data of users from major tech companies like AOL, Apple, Facebook, Google, Microsoft, Paltalk, Skype, Youtube and Yahoo.



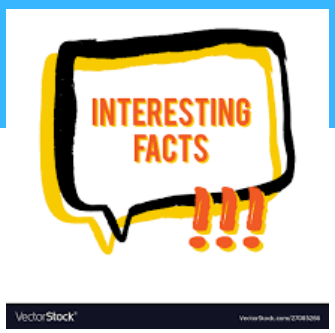
The NSA also collects data from telecom companies like Verizon, Sprint and AT&T. The GCHQ, British equivalent of the NSA, has the terrifying ability to actually control people's phones, even when they're switched off, using their Smurf suite.

- Dreamy Smurf – Has the ability to turn phones on or off remotely
- Nosey Smurf – Has the ability to make use of the phone's microphone to listen to conversations and noise in the local area
- Tracker Smurf – Has the ability to precisely track your position
- Paranoid Smurf – Works to hide the activities of the other Smurfs to prevent detection

XKEYSCORE (XKS), is a system designed to search and analyse internet data from users all over the globe. The GCHQ Tempora is another computer system that uses various surveillance tools to hack into fibre optic cables and connections all over the globe. The Boundless Informant tool keeps track of all metadata collected by the NSA and makes a 'heatmap' of that data to show where it came from and which countries are targeted most often. In addition to this, Snowden's files also revealed that the NSA has targeted global leaders. Dilma Roussef, Felipe Calderon and Angela Merkel have all been victims of the NSA's surveillance. The Bullrun system is designed to crack widely-used encryption and security measures using different hacking tools in order to break through standard encryption systems like HTTPS and SSL.

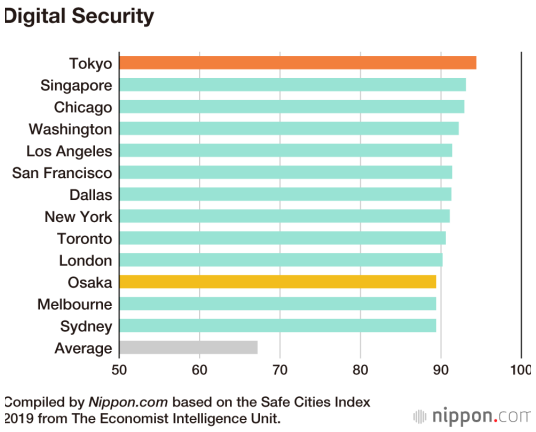
What if the world Governments, aided by big internet companies, are working to create a permanent record of everyone on Earth, secretly documenting their daily lives? If even the biggest internet companies on the planet can be hacked into with such apparent ease, is anyone really safe?

References: https://www.csoonline.com/



INTERESTING FACTS

- Tokyo is the most cyber-secure city in the world.



- Kevin David Mitnick is the world's most renowned hacker. Beware of him!

- There is a successful hack somewhere on Earth every 39 seconds.
- Wireshark is the the most popular and widely used network protocol analyzer and is an important security application.
- Phishing sites have a life cycle of about 15 hours. Google, PayPal and Apple are the most commonly spoofed organisations.

References:

https://www.cybintsolutions.com/

INTERNET SAFETY WHILE BROWSING

BY SHYAMA HARIHAR

The world we live in today cannot be compared to that from the past. Each sunrise comes included with an advertisement of a new mobile phone with eye catching, state of the art features. New application software are launched every now and then to serve the people. Most people are unaware of the hidden dangers of using a new mobile phone purchased with their hard earned money after several time consuming visits to shops. The next decade will surely usher in much more faster devices with more RAM and with high internal memories like 256 GB as a starting point.

Take for example, one of the most used features on the Internet: the God send - mobile banking which has become the first priority for all of us. Thus, the internet is indelibly and directly linked to financial safety which is of paramount importance to every person. There can be no two opinions about the fact that the common man has to be educated through audio visual media about the safety of the Internet for when he browses it to attend to his daily functions.

There can be no two opinions that login IDs and passwords are prerequisites in gaining access to a computer. In the case of a mobile phone, pattern locks or facial unlocking can be used. Below are a few points summarized for people to be aware of their online safety and wellbeing.

- To protect one's personal identity, login ID, password, etc., the user has to perform individual and independent browsing.
- It is to be ensured that a working and up to date anti virus service is operational.
- When using means of public transport like airports or railway stations, it is better to avoid important and sensitive browsing on public WiFi access points.

- For extremely sensitive and secretive work, there can be no doubt that the desktop computer shall not be connected to the Internet at all. One should also remember to physically prevent access to USB ports by taping them up with cellophane tape to ensure USB devices are not plugged in by mistake. The classic example of the Stuxnet virus developed by the CIA of USA can be taken as the perfect illustration. The virus was used to slow down or destroy the illegal Iran Nuclear Weapon programme. It is widely believed that the virus hit the illegal facilities and then got transmitted world over when an Engineer used an infected pen drive on his laptop which was connected to the local network at the facility. Billions of rupees were spent world over, to combat the CIA engineered virus. Thus, issues involving national security, industrial secrets, scanned secretive records, research papers etc., need to be secured in standalone offline computers.

- The user can opt to browse in incognito mode which promises no history tracking. However, the user should also have a safe network connection. Furthermore, he should ensure that no one is peering into his screen in some way.
- Spyware is another area which is alarming to say the least. The user shall decide wisely when he uses free websites. Freebies are offered as a trap. E-books, music, movies, you name it all, the trap can be anywhere.
- Desktops shall not be left unattended when logged into. If doubtful, the Gary McKinnon case can serve a point. He even cracked USA defense websites. Thus, the individual has no choice but to be alert.
- The user shall operate the delete history option from the beginning of time. If there is a poser, pray tell us, how many times do we use to refer browsing history for ourselves...
- Finally, shut down the computer when you leave for home or when you go to bed. Night time, when the world sleeps, is also when hackers excel, just like foxes and wolves.

What factors make people successful in cyber security?

1.Strong technical knowledge

2.Ability to learn and research new information.

3.Logical reasoning , troubleshooting

4.Ability to lead a project (leadership qualities)

5.Verbal communication for customer services

6.Ability to work independently

1.**TROY HUNT**:

He is an eminent security expert and has been named Microsoft's most valued professional in developer security. He created a HIBP project which is a free data breach service that allows people, both technical and non technical, to determine whether they are impacted by a data breach whether and their personal information is compromised. This service has 8 billion records.

2.**BRAIN KREBS:**

He worked as an investigative journalist. He has his own security blog named as KrebsOnSecurity .This blog has got much appreciation because it includes posts on uncovering cyber criminals and has reported first on several high profile data breaches or Home depot.

3.**JOHN MCAFEE:**

He worked for numerous tech companies even for NASA. He built a company which came up with the first commercial antivirus software for personal systems which turned out a great success and gained a large user base.

4.**EUGENE KASPERSKY**:

He co-founded and is the current CEO of Kaspersky Labs, which is one of the largest endpoint securities companies in the world. They develop security solutions, and their antivirus software is used commercially and by many Governments across the world.

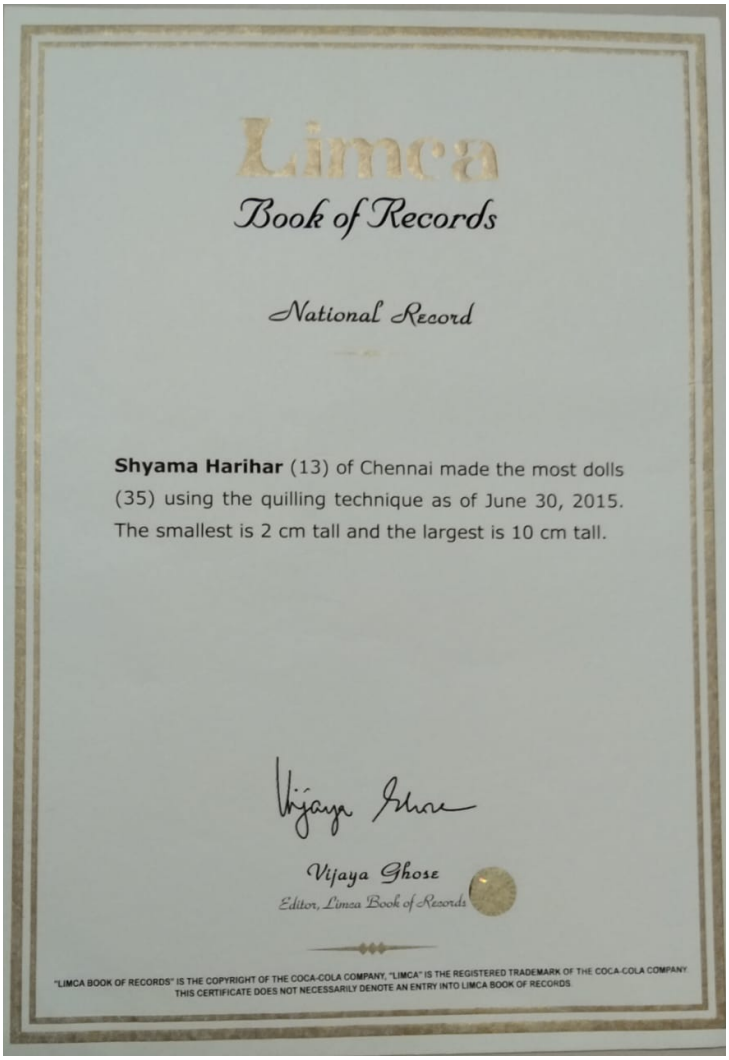
Troy Hunt

Eugene Kaspersky

References:

1.https://startacybercareer.com
2.https://dice.com

Student Achievements


Limca
Book of Records

National Record

Shyama Harihar (13) of Chennai made the most dolls (35) using the quilling technique as of June 30, 2015. The smallest is 2 cm tall and the largest is 10 cm tall.

Vijaya Ghose
Editor, Limca Book of Records

"LIMCA BOOK OF RECORDS" IS THE COPYRIGHT OF THE COCA-COLA COMPANY, "LIMCA" IS THE REGISTERED TRADEMARK OF THE COCA-COLA COMPANY. THIS CERTIFICATE DOES NOT NECESSARILY DENOTE AN ENTRY INTO LIMCA BOOK OF RECORDS


Just for the record

Passion And Skill Apart, Extensive Research And Smart Planning Are Needed To Enter Halls Of Fa

C Suresh

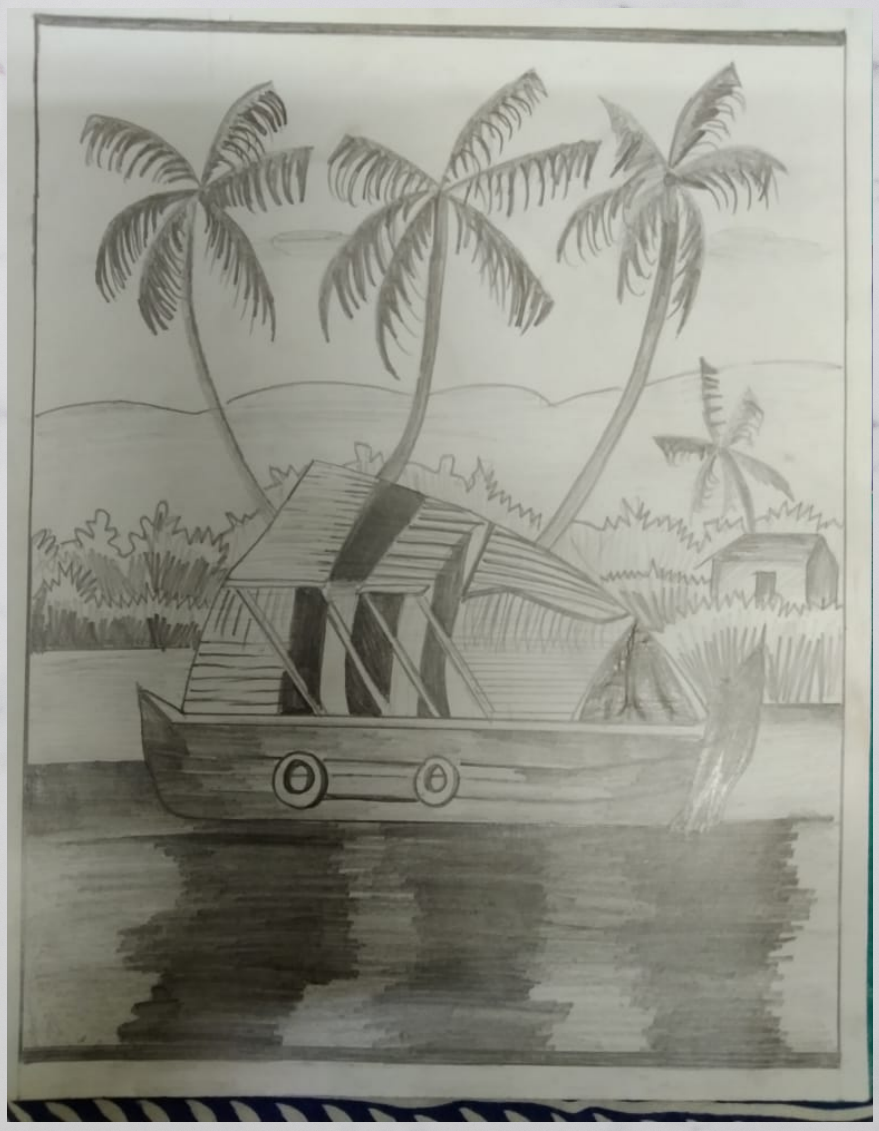
IN THE SPOTLIGHT: Shyama Harihar, 15, quilled 35 miniature cartoon characters and entere the Limca Book of Records

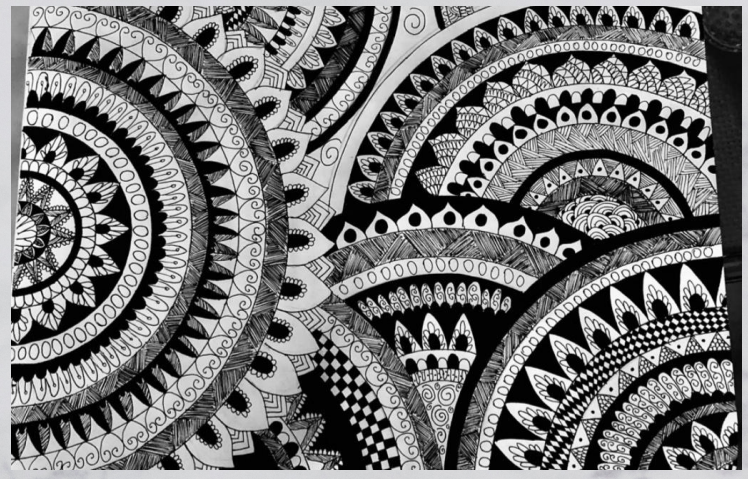
Shyama Harihar of CSE-B is a Limca Record Holder in the field of Quilling. She was a twelve-year-old schoolgirl when she first came across quilling tools in a stationary shop. She visited that shop for buying her usual high-end pens, when her curious eyes seemed to light up and sparkle at the sight of some of the other items up for sale. She asked the shop owner about them, and was told they were quilling tools. Thus started her journey into the world of quilling. After arduous efforts of self-learning courtesy YouTube, she made her first quilling items. She would often stare with awe at the excellent quilling skills of some and questioned whether she'd be able to produce art of similar quality.

Coloured strips of quilling paper, the priceless quilling tools, a focussed mind eager to learn new things and a pair of deft hands, all helped her make plenty of quilled objects.She made colourful earrings, cartoons including characters from Mickey and Minnie mouse and the Doraemon series as well as wildlife like owls and much more. The undaunted support of her parents stood testament to their belief in her. Then an idea struck at the age of thirteen to make an application for claim in the esteemed Limca Book of Records. From their website, phone numbers and email id were gathered. Following instructions, images were sent for their scrutiny and approval. This was followed by further verification by the team at Limca. There was no word from the Limca authorities for a long time. One day, on returning from shopping, she was handed over a light grey envelope by the gate security. It had arrived by speed post. Printed on the exterior of the envelope was the word Limca. It was a pleasant surprise. On opening the envelope at home, she was elated and was on cloud nine to see the original title of Limca Book of Records for quilling at the age of thirteen for making 35 dolls. Without arts, literature, sports, music and drama, this world would be colourless and opaque, and let's not forget the fact that it would be bereft of ethics and values. Shyama Harihar would definitely focus further on art appreciation. This may well be one of those areas, where single minded pursuit and devotion can set records which are truly written in letters of Gold.

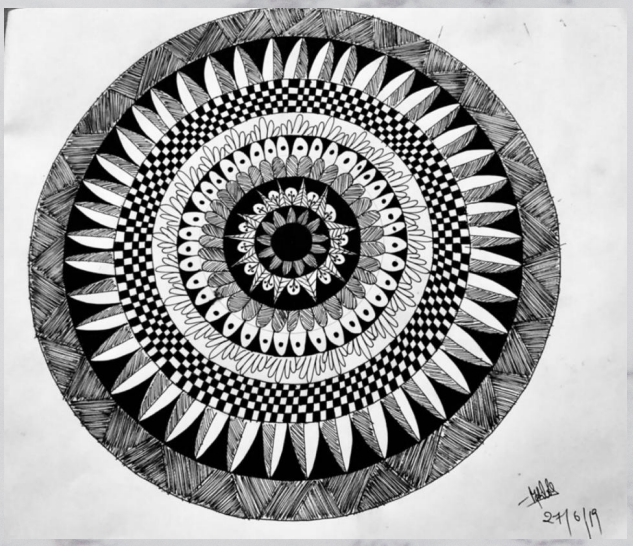
Student's Contribution

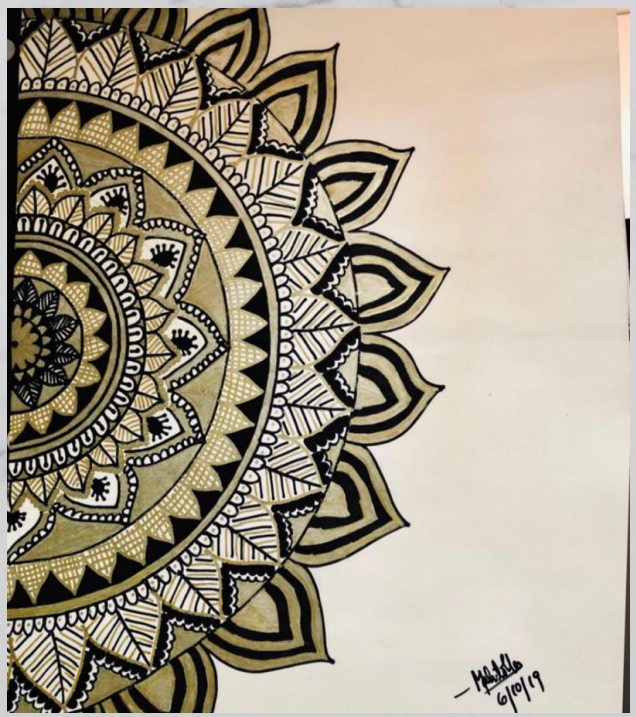
Shyama Harihar

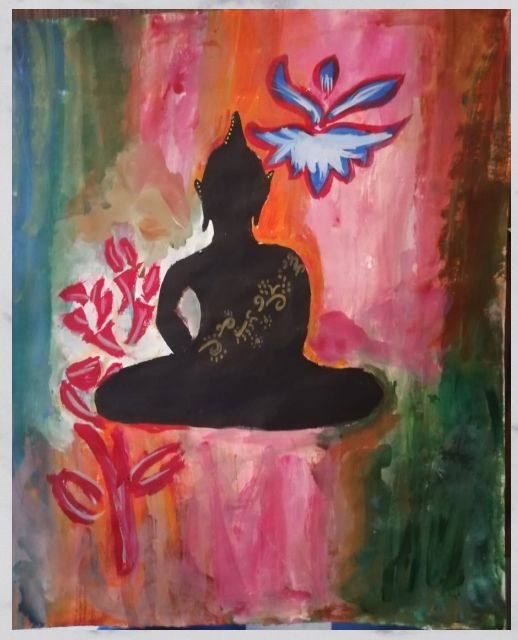




MAHIMA LOLLA







SNEHA

இதயத்தை நிரப்பியவளே !

மொழியின் தொடக்கமே !
பாரதத்தின் நாடித்துடிப்பே !
தமிழ்தாயே !
திருக்குறளால் உலகே வியந்தவளே !
திருவையாற்றில் பக்தி கண்டவளே !
பரதத்தில் பாவனை புகுத்தியவளே !
பாரதியின் பிறப்பு கண்டவளே !
ஜல்லிக்கட்டில் வீரம் சொன்னவளே !
கட்டபொம்மனின் சுதந்திரதாகம் உணர்ந்தவளே !
சோழர்கோவிலில் கணிதம் கண்டவளே !
கோபுரகலசத்தில் அறிவியல் கண்டவளே !
உழவினை உடுத்தியவளே !
தலைவாழையில் விருந்தோம்பல் செய்தவளே !
கோலத்தில் கலையினை கண்டவளே !
பாரம்பரிய உணவுச்சுவையில் திளைத்தவளே !
சித்தமருத்துவத்தின் சிறப்பை உணர்த்தியவளே !
மரப்பாச்சியில் மருத்துவம் வைத்தவளே !
கல்லணையில் சரித்திரம் பொறித்தவளே !
காஞ்சிபட்டில் காவியம் படைத்தவளே !
தாலாட்டில் பாசம் புகட்டியவளே !
பண்பாட்டில் உச்சம் தொட்டவளே !
கலாச்சாரத்தின் கருவறை நிறைத்தவளே !
அன்னைமடியின் அர்த்தம் சொன்னவளே !
இலக்கியத்தின் இலக்கணமே !
நாகரீகத்தின் தொப்புள்கொடியே !
தாயே தமிழ்தாயே
வணங்குகிறோம்

சங்கீர்த்தனா பாலசுப்ரமணியம்

FACULTY COORDINATORS

Dr. D. Venkataraman

Mrs. T. Bagyammal

Mrs. R. Archana

ASCII executive members:

Sai Priyadharshini (IV year)

Adithi Narayanan (III year)

Roopa Vidhya (III year)

Editor:

Shyama Harihar (II year)

Acknowledgement to:

T Selva Sanjana (II year)

Nirmal Karthikeyan(II year)