

PREVIEW PREVIEW PREVIEW PREVIEW

eForensics

VOL. 11

NO. 10

Wilson Mendes

18 ARTICLES!
200 PAGES!
1 AUTHOR!

THE ESSENTIAL GUIDE TO CYBERSECURITY CHALLENGES

UNDERSTAND
WHY
ENCRYPTION
IS IMPORTANT
FOR
PROTECTING

DISCOVER
THE SECURITY
RISKS RELATED
TO **WIRELESS**
COMMUNICATION
AND WIF

LEARN ABOUT
THE METHODS
USED BY
FORENSIC
EXPERTS IN
SMARTPHONE

FIND OUT
HOW TO
SAFELY
HIDE DATA
USING
STEGANOGRAPHY

PREVIEW PREVIEW PREVIEW PREVIEW

ISSN 1733-7186

EDITOR'S WORD

Dear Readers,

This special compendium of Wilson Mendes' latest technical articles will take you on a fascinating journey through the complexities of cybersecurity, forensics, and information protection. "I hope these articles inspire and enrich your understanding of digital security and forensics issues, as well as the work I have dedicated to research and knowledge sharing."

In this special edition, we include an interview with Wilson Mendes to offer an insight into his experiences, routines, philosophies, and the journey that led him to become a respected professional in the field of information security. "I believe sharing knowledge is key, and I am always excited to learn and grow alongside the security community."

In my role as a researcher and penetration tester with Red Team, I read books and technical articles, developed and experimented with new tools, kept up to date with cybersecurity trends, and looked at offensive and defensive areas.

In 'The Wilson Mendes Compendium', articles will cover a variety of topics, including malware, obfuscation, operating systems such as Windows, Linux, and BSD, machine learning algorithms, cryptography, backdoors, telephony, and secure communications.

"Information is a common good that cannot be monopolized." I hope these articles inspire your explorations and discoveries in the vast landscape of information security. I look forward to continuing to share my knowledge and experience with the community while learning from you at the same time.

Yours sincerely,
Wilson Mendes, Ewa Dudzic, and eForensics team

ewa.dudzic@eforensicsmag.com

AUTHOR'S WORD

Dear Readers,

I hope this message finds you well. I would like to share with you a brief insight into the articles I have recently written for eForensics Magazine, as well as what readers can learn from them.

18 articles cover the technical aspects in depth while developing the articles in a language that supporters of the hacker universe can understand.

I believe this special edition compilation represents an opportunity to add value to the magazine's subscribers by bringing a collection of valuable pieces of knowledge into the digital universe.

All of these articles provide our readers with the opportunity to gain comprehensive knowledge on cybersecurity issues, forensic investigation, and personal information protection. Each article provides a unique and practical perspective on the challenges and solutions in these critical domains.

We appreciate the opportunity to discuss these topics with our readers and look forward to continuing to provide useful information in our magazine.

Yours sincerely,
Wilson C.S Mendes



Cover Image
Wiktorja Bukowska

Cover Design
Wiktorja Bukowska

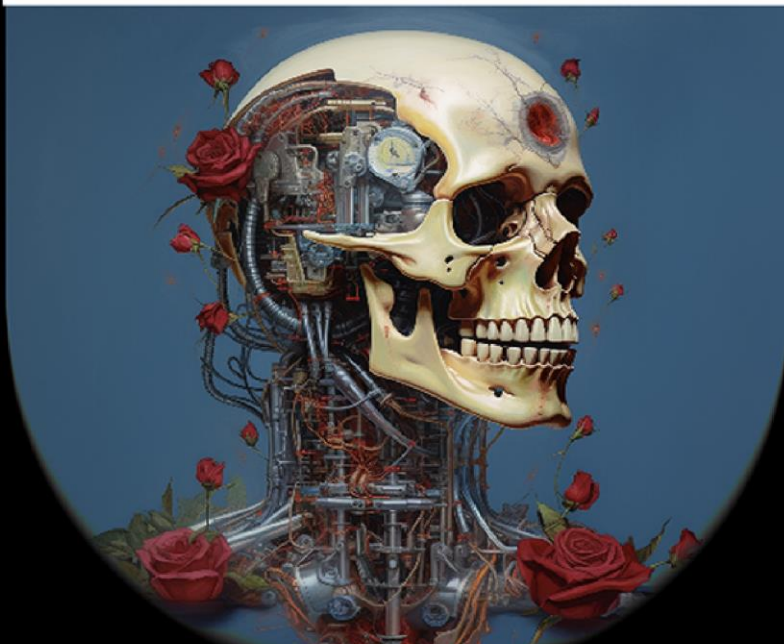
06	INTELLIGENT ALGORITHMS AND FORENSIC INVESTIGATION: THE MEETING BETWEEN SHERLOCK HOLMES AND THE DIGITAL AGE
18	CRYPTOGRAPHY AND THE FRONTIER OF PRIVACY
36	PRIVACY? 404 PAGE NOT FOUND
51	FORENSIC INVESTIGATION IN DOCKER ENVIRONMENTS: UNRAVELING THE SECRETS OF CONTAINERS
85	STEGANOGRAPHY – A HIDDEN REALITY FAR BEYOND WHAT THE EYES CAN SEE
94	INTERVIEW WITH WILSON MENDES
98	RANSOMWARE – ATTACKS ON THE RISE: ARE WE PREPARED FOR THE NEXT WAVE OF CYBERCRIME?
107	DATA FOR SALE: THE COMMODITIZATION OF PERSONAL INFORMATION IN A CONTROLLED SOCIETY
118	INSTAGRAM: THERE IS SOMEONE BEHIND THE DOOR
124	DANGEROUS IS IN AIR
132	FORENSIC INVESTIGATOR MOBILE IN THE LOST WORLD OF CRIME
139	CATCH ME IF YOU CAN
148	THERE IS HONOR AMONG THIEVES
162	FORENSIC TOOLS? ELEMENTARY, MY DEAR WATSON
170	HOW TO MAKE CYBERSPACE SAFE?
177	MALWARE – THE NIGHTMARE TIME
184	STEGANOGRAPHY – PROTECT YOUR DATA
188	MOBILE SERVICE BREACH-BEHIND THE SCENES WORK

All trademarks, trade names, or logos mentioned or used are the property of their respective owners. The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

GET YOUR COPY NOW!

eForensics | VOL. 11
NO. 09

ISSN 1733-7166



**THE COMPLETE GUIDE
TO USING AUTOPSY**

LEARN HOW TO PERFORM A FORENSIC ANALYSIS USING AUTOPSY 4.21.0	EXPLORE HOW TO USE AUTOPSY, FROM STARTING A CASE TO MANAGING ARTIFACT CONTENTS	HUNT HACKERS USING AUTOPSY ON A MACOS IMAGE	USING AI AND HIGH-TECH TOOLS , REDEFINE THE LIMITS OF CASE SOLVING
--	---	--	---

]WITH THE HELP OF ALL THIS KNOWLEDGE, YOU WILL BE ARMED TO SOLVE EVERY CASE AND RANK AMONG THE INDUSTRY'S TOP EXPERTS.

INTELLIGENT ALGORITHMS AND FORENSIC INVESTIGATION: THE MEETING BETWEEN SHERLOCK HOLMES AND THE DIGITAL AGE



"It's not what you know, but what you can prove." Anonymous

CRYPTOGRAPHY AND THE FRONTIER OF PRIVACY

"Security is a process, not a product." Bruce Schneier



Cybersecurity has emerged as one of the most pressing and complex challenges facing contemporary society. The growing interdependence of systems and reliance on digital data has made protecting information and ensuring the integrity of online communications imperative for businesses, government organizations, and individuals.

In this context, cryptography, through mathematically robust algorithms and advanced techniques, stands out as a fundamental pillar of social defense, providing the essential mechanisms to preserve the confidentiality, authenticity and integrity of static and dynamic data, allowing the codification of the information, making it unreadable for any unauthorized person.

This article seeks to provide an in-depth exploration of the applications of cryptography in the context of cybersecurity. We'll cover a variety of complex and essential topics, including symmetric and asymmetric key cryptography, encryption algorithms, authentication protocols, digital signatures, and key management. In addition, we will examine practical use cases where encryption plays a critical role in mitigating cyberthreats, such as man-in-the-middle attacks, data tampering and identity theft, and the contradiction with GDPR and LGPD regulations that have angered governments and law enforcement.

Introduction



"Privacy for the weak and transparency for the powerful." Julian Assange

PRIVACY? 404 PAGE NOT FOUND

“Who controls the past, controls the future; who controls the present, controls the past.”
George Orwell



Introduction

In recent years, remote video identification has been a topic of great interest in the current context of surveillance and security technologies, becoming a technology increasingly used around the world. Through advanced recognition algorithms, surveillance systems designed for different purposes, such as access control, criminal investigations and real-time monitoring, allow identification systems to be implemented. As a result, images captured by security cameras and posting on social networks form part of this identification tracking. This technology, while having several advantages, also raises concerns regarding privacy and the risk of increasing social inequalities.



In this article, we delve into an identification and scoring system, sifting through images of people, exploring concerns raised and analyzing the two main methods of identification and video surveillance around the world. We then discuss some of the advanced algorithms used to identify and recognize objects, activities, marks and faces in videos.

Video Recognition Systems

There are several types of video recognition systems in the world. Some of the main ones are:

Facial Recognition System: These systems use advanced algorithms to identify and recognize faces in videos. They are widely used in security and surveillance, access control and even in social networks for automatically tagging people in photos and videos.

Recognition System: These systems are able to identify and classify objects in videos. They can recognize different types of objects such as cars, animals, buildings, among others. These systems are used in applications such as traffic surveillance, in-store customer behavior analysis, and object detection in security videos.

Action Recognition System: These systems have the ability to recognize and interpret actions and movements in videos. They can identify human activities such as walking, running, lifting objects, dancing, among others. These systems are used in areas such as forensic video analysis, monitoring behavior in public spaces, and analyzing sports performance.

Brand Recognition System: These systems are designed to identify and recognize brands, logos and symbols in videos. They are used in advertising, media analysis and marketing to monitor the presence and exposure of brands in different contexts.

One of the most well-known and controversial video remote identification systems is the one used in China. The Chinese government has implemented a mass surveillance system that uses advanced facial recognition algorithms to track and identify its citizens. In addition, it associates a social score to each individual, based on their behavior and activity history. This system, according to the government that uses it as a justification to monitor the citizen, aims to create a safer and more disciplined society, but at the same time raises serious concerns regarding privacy and human rights.

The remote video identification system implemented by the Chinese government is known as the "Social Credit System" and is a core part of China's "Mass Surveillance" initiative. This system combines surveillance cameras with advanced facial recognition technologies, artificial intelligence and big data to monitor, track and identify citizens in real time.

FORENSIC INVESTIGATION IN DOCKER ENVIRONMENTS: UNRAVELING THE SECRETS OF CONTAINERS



*"Criminals always leave evidence in their actions."
Edmond Locard*

The story of Noah's Ark, widely known as a biblical account, can be related to the context of Docker technology. Just as Noah was instructed to build the Ark to house his family and divide it into compartments to accommodate all species of animals, similarly, Docker provides a container platform that allows you to create and isolate environments for applications and services using a specific configuration, such as the Dockerfile, and organize these containers into separate networks and volumes.

As the Ark protected its occupants during the flood, Docker provides isolation and security for applications and services running in containers. Each container is encapsulated, ensuring that an application's dependencies and configurations do not affect other containers running in the same environment.

The Ark represented salvation and hope in the midst of destruction; Docker represents a modern solution for deploying and managing applications in complex environments. With Docker, you can quickly build and deploy consistent environments across different operating systems and infrastructures, making it easier for development and operations teams to collaborate.

The benefits offered by Docker in the current technological context teach us about the importance of protection, cooperation and preservation.

Introduction

Docker has become a popular container platform, revolutionizing application development and management. However, this innovation also brought challenges in the area of forensic investigation. Docker containers offer flexibility and efficiency in packaging and deploying applications, but it's important to recognize that they can also be vulnerable to security incidents, just like any other computing environment.

In this article, we'll explore the fascinating world of forensics in Docker environments, revealing the essential techniques and tools to unlock the secrets hidden in containers. We'll cover analyzing Docker containers, detecting malicious activity, gathering evidence, and investigating incidents.

Disclaimer

This article is a comprehensive source of tips and tricks for Docker system protection and forensics. In it, we explore the ins and outs of this technology, offering valuable insights and scripts for asset resolution, optimization and protection.

While it would be ideal to divide the article into three parts to address all forensic analysis possibilities, we are aware that time is limited. However, our intention is to provide the most relevant information to facilitate forensic analysis of the Docker environment, covering a wide range of possibilities.

Feel free to explore the techniques and tools shared in this article, and we hope you find useful resources for improving security and forensics in your Docker projects.

That's all folks!

I. What is Docker and why is it important for digital forensics?

Docker is an open-source platform that allows you to build, distribute and run applications in isolated containers. These containers are self-contained, lightweight, portable units that encapsulate all of the components needed to run an application, including code, libraries, and dependencies. Docker technology has revolutionized software development and deployment, providing greater efficiency, scalability, and consistency. However, the ephemeral nature of Docker containers presents specific challenges for digital forensics. Unlike traditional virtual machines, Docker containers do not have a complete operating system, which makes evidence collection and forensics difficult. Furthermore, the dynamics of containers, such as rapid creation, modification, and destruction, add to the complexity of investigations.

STEGANOGRAPHY - A HIDDEN REALITY FAR BEYOND WHAT THE EYES CAN SEE

"A PICTURE IS WORTH A THOUSAND WORDS" CONFÚCIO

IT'S TRUE?



Art by <https://www.linkedin.com/in/geizabarreto/>

Start

Steganography is an ancient secret communication technique that consists of hiding messages within other means of communication, such as images, texts or physical objects. The term "steganography" derives from the Greek words "steganos" (hidden or covered) and "graphein" (to write), reflecting its nature. Its use dates back to antiquity, with historical records that indicate its existence since ancient times. A documented example is the scraping of wax from a wooden tablet to hide a message, allowing only those who knew the method to retrieve it.

During the Middle Ages, steganography was widely employed for military and espionage purposes. The invisible ink technique was especially notable, using a special ink that could only be revealed through specific chemicals or heat. This technique was commonly used to convey secret information in letters and documents. With the advancement of technology, steganography has evolved and found new applications. During World War II, for example, even with the different ways of encoding messages used at the time, the technique was used to hide information within other types of communication, such as images or radio transmissions, making it difficult for the enemy to detect and decipher it.

In the digital age, steganography has become even more relevant. Nowadays, it is often used to hide sensitive or confidential information in media files such as images, videos and other digital files. This information can range from secret messages to copyrighted files.

Steganography has a long history, from its use by the ancient Greeks to its contemporary application in the digital age. It remains a powerful tool for covert communications and data protection, with its development and evolution closely linked to the advancement of technology and security needs over the centuries. I invite the noble reader to embark on this technological journey of a past that is increasingly present in our lives, revealing an increasingly complex future in secret communication.



In the information age and digital communication revolution, Internet and cloud services are widely used in transmitting large amounts of data through social media, like Facebook, Instagram, WhatsApp and various other insecure networks, exposing secret data, thus creating thousands of victims, generating serious situations. In addition, new technologies and new applications, such as the Internet of Things (IOT) and artificial intelligence (AI), which are increasingly used, bring new threats.

To keep unauthorized people, spies, telephone operators and authoritarian governments away from the transmitted information, a variety of techniques have been introduced ensuring that the transmission of information through these means is safer and more secure, making it one of the most important issues in the field of data security. and steganography is one of them. Steganography as a secret communication technique aims to hide secret messages in a normal message, obtaining as little detectability statistics as possible and without raising suspicions during data communication.

Steganography differs from other data security techniques. A simple conceptual diagram representing the general process of steganography.

INTERVIEW

WOULD YOU KINDLY INTRODUCE YOURSELF TO OUR READERS?

Hello world!

My name is Wilson Mendes and I am an Information Technology (IT) professional specializing in Information Security with extensive experience in various areas including cybercrime, artificial intelligence, cryptography, firewall and data security. My experience also covers Malware, Reverse Engineering, Chatbot, Crawlers, Commercial Automation, Microservices and Embedded Systems. I have in-depth knowledge of security protocols, privacy and anonymity, network administration and Linux systems, FreeBSD (my eternal passion), NetBSD and OpenBSD.

Throughout my career, I have worked as a consultant, focused on cybercrime prevention, forensic investigation, reverse engineering, cryptography deployment, ISO/SCADA standards adoption, ethical hacking, network auditing and distributed malware detection systems. I also participated in the adequacy and implementation of artificial intelligence and security devices, developing anti-tracking devices and ensuring secure transactions on public networks through the elaboration of risk and failure containment plans.

I currently work as a Pentest Red Team member and actively contribute to the dissemination of knowledge in the area through lectures, interviews and articles in reputable magazines, such as eForensics Magazine and Hakin9 Magazine.

PLEASE ELABORATE ON YOUR DECISION TO WORK IN THIS FIELD.

Since I was a child, I've always been passionate about electronics, televisions, portable radios, recorders... I've always been curious about how these objects worked, I wanted to know what each electronic device was for, their respective functions. When I had contact for the first time with walkie talkies, it was love at first sight, I was curious how that communication was possible, including the capture of cordless phone frequencies, amateur radio and other noises that left me fascinated by a universe of discoveries that lay ahead. When I had contact with my first computer at the age of 13, a TK-3000 was an explosion of feelings. Programming in Basic, recording the information on cassette tapes and soon after programming for 5.25 floppy disks. That's how it all started.

WHAT IS YOUR TYPICAL DAY AS CYBERSEC ENGINEER?

I'm a very disciplined person, I wake up every day at 4:40 am, I go swimming four days a week, then I drink a special coffee balanced with tropical fruits. I start my professional day by checking the agenda with the tasks I have to accomplish. I almost always use headphones to listen to music or sound frequencies that increase my concentration power.

I practice the pomodoro technique when I'm working, so every 50 minutes of work, I confess that sometimes the idea flows in such a way that I can't get up from the computer, but when possible, in an interval of 10 minutes per hour, I do stretching on the ball or on the mat, I also use a massage chair along with a foot massage, to generate comfort for long-term work. I take a break for lunch, which is usually from 12:30 pm to 1:30 pm, I return to the chore routine at 2:00 pm, continuing until 6:00 pm. At night, I practice weight training five days a week. After showering, I have a light meal. And soon after, I pray and meditate not to take with me any tasks or memories of the day before bed.

WHAT METHODS OR EQUIPMENT DO YOU EMPLOY AT YOUR JOB?

I use pomodoro for time control, Jira for scheduling and projects, Tasknote for notes related to routines. A notebook and pen to ensure the information is safe (backup, lol). Equipment related, I use two Lenovo i7 notebooks with 32GB RAM, 2TB and advanced encryption and a desktop with razer processor and 64GB of RAM with four SSDs of 2TB for work.

WHICH TOOL IS YOUR FAVORITE?

It depends a lot on what I'm going to do, but I can mention some that I believe are like a Lego game, they fit into each other, but **ReconFTW** is without a doubt a kind of Swiss army knife. However, it has: Arachni, Sniper, Naltgeo, Netcraft, Metasploit, Nessus, HyperionNul Evasion, Nmap, Wireshark, Burp Suite, Nuclei Crackmap. As for the wireless network, my favorites are: Aircrack-ng, Kismet, Wi-Fi Cracker, Reaver, Bully, WiFite, PixieWPS, Linset, NetStumbler. But my current favorite is Flipper zero.

YOU HAVE EXTENSIVE EXPERIENCE AND KNOWLEDGE ACROSS A WIDE RANGE OF TOPICS. YOUR ARTICLES ARE VERY INFORMATIVE FOR OUR READERS. WHAT ARE YOUR CURRENT THOUGHTS ON CYBER SECURITY? WHERE ARE WE?

First thank you very much for your comments. It is always a great honor for me to be able to write for an encyclopedia that brings together great writers. As study is routine in my life, knowledge is something continuous. The field of security continues to grow, and so exponential growth will continue forever. Information security is something very complex, because between system and hardware failures and human errors, there are gaps and that's exactly where the opportunity arises, multiplied by zettabytes of information exposed for free on the internet, for good or for evil, made accessible for everyone.

Add to this the internet of things and artificial intelligence, which is increasingly accessible and popularized, and accelerates every day with hundreds of interactions between machines and human beings, making learning about any subject become superior to any outdated, primate and traditional teaching method. As the principle of economics is based on the law of demand and supply, there is a universe of possibilities that is increasingly enhanced by new technological ruptures. We are in a transition where the old and primitive way of learning will certainly end. What is happening is a transformation that involves the entire globe and those countries, governments, social sectors that are not prepared will be left behind.

WHAT ARE THE MAIN TACTICS YOU'VE OBSERVED BAD ACTORS EMPLOYING LATELY?

This depends a lot on the scenario, the target to be attacked. But there are patterns to reach the objective, and the consequences of this depend on the answers that these techniques and tactics manage to extract. I could cite some such as: Social engineering, Distributed Denial of Service (DDoS) attacks, Phishing, Advanced Persistent Threats (APTs), Identity theft, Malicious software distribution, Ransomware attacks.

It is important to be aware of and keep up with the latest security practices to mitigate the risks associated with these tactics. Additionally, consulting up-to-date sources and security experts will provide more accurate and timely information on current tactics employed by authoritarian governments, spies, hackers, and rogues.

IS THIS A PARTICULARLY EFFECTIVE TACTIC IN YOUR OPINION?

Yes, phishing is considered to be an effective tactic employed by malicious people. It has been widely used for many years and continues to be a prevalent threat. Phishing attacks can be successful because they exploit human vulnerabilities such as trust, curiosity or urgency to trick individuals into taking actions that compromise their security.

Phishing emails or messages often appear genuine, mimicking the branding and language of legitimate organizations or individuals. They can create a sense of urgency or offer attractive incentives to prompt users to click on malicious links, provide personal information or download infected attachments. This can lead to various harmful outcomes such as identity theft, financial loss, unauthorized access to accounts or installation of malware.

The success of phishing attacks often relies on social engineering techniques, psychological manipulation, and careful impersonation of trusted entities. Malefactors continually adapt their strategies, making it difficult for individuals and organizations to identify and defend against these attacks effectively.

To mitigate the effectiveness of phishing attacks, it is crucial to make users aware of the characteristics of phishing emails, teach them to identify possible warning signs, and educate them on online security best practices. Employing email filters, multifactor authentication, and keeping software and systems up to date are additional measures that can help combat phishing attempts.

WHAT'S THE BEST DEFENSE AGAINST MALICIOUS INSIDERS?

Defending against malicious persons within an organization who abuse their authorized access for harmful purposes is a major challenge.

With some basic requirements, we will be able to increase and improve the defense system.

- 1- Strict Access Control: Implement a robust system of access controls and permissions that restrict employee access to confidential information or critical systems based on their job roles and responsibilities.
- 2- Principle of Least Privilege: Adhere to the principle of least privilege, granting employees only the minimum level of access necessary to perform their job duties.
- 3- Monitoring and Auditing: Establish robust monitoring and auditing systems that track user activity, access logs and changes to critical systems or data.
- 4- Segregation of Duties: Implement the separation of duties so that critical tasks require the collaboration of multiple individuals.
- 5- Employee Education and Awareness: Conduct regular training and awareness programs to educate employees about the risks associated with insider threats and the potential consequences of their actions.
- 6- Incident Response Plan: Develop a comprehensive incident response plan that includes specific procedures for dealing with insider threats.
- 7- Non-Disclosure Agreements and Background Checks: Implement robust hiring processes that include thorough background checks and screening of potential employees.
- 8- Promote a positive work environment: promote a positive work environment that encourages open communication, trust and transparency. Employees who feel valued and supported are less likely to engage in malicious activity.

While it is challenging to completely eliminate the risk of malicious intruders, implementing a combination of these strategies can significantly increase an organization's ability to detect, deter, and respond to these threats.

DO YOU HAVE ANY ADDITIONAL SUGGESTIONS FOR IMPORTANT CYBERSECURITY FOCUS AREAS?

These are the areas that I believe are already growing exponentially.

- Cloud security is of paramount importance as organizations increasingly adopt cloud computing services. In this context, it is crucial to ensure the security of cloud environments, which involves implementing appropriate access controls, encryption, monitoring and regular vulnerability assessments of cloud infrastructure and services.
- Internet of Things (IoT) security has also become a significant concern due to the proliferation of connected devices in homes, businesses and critical infrastructure. Expertise in IoT devices, networks, and data, including strong authentication, encryption, and patch management, is critical to ensuring security in this context.
- Additionally, the security of Artificial Intelligence (AI) and Machine Learning (ML) is an important consideration as these technologies are being integrated into many applications. Addressing areas such as adversarial attacks, data poisoning, and the ability to explain the model need to be addressed to ensure the security of these systems.
- Privacy and data protection are essential aspects to be considered. It is critical to protect user privacy and comply with data protection regulations such as GDPR and CCPA. In this regard, organizations should implement strong data protection measures such as encryption, data minimization and privacy by design principles.
- Mobile security is also crucial given the widespread use of mobile devices. To secure mobile apps and devices, it is important to implement mobile device management (MDM) practices, strong authentication, and secure encryption in order to mitigate threats related to mobile devices.
- Finally, performing security testing and vulnerability management on a regular basis is a fundamental practice. This involves performing penetration tests, vulnerability assessments and implementing a robust patch management process, allowing for effective identification and treatment of vulnerabilities. Remember that cybersecurity is an ongoing and evolving process. It's important to stay current with emerging threats, technology trends, and best practices to ensure a strong security posture.

WHAT ARE YOUR THOUGHTS ON AI, THE CURRENT TRENDING ISSUE? WHAT DIRECTION DOES IT LEAD US IN?

In my opinion, Artificial Intelligence (AI) is a powerful and transformative technology that is advancing rapidly and disrupting many social sectors. It has the potential to revolutionize society in areas such as health, transportation and education. AI has already demonstrated its capabilities in image and speech recognition, natural language processing and autonomous systems.

A current AI trend is the impact on the workforce and job displacement. Automating tasks through AI raises concerns about possible job losses in some industries. However, AI can also create new job opportunities and transform existing roles. To adapt to these changes, it is important to develop new skills and promote continuous learning.

The ethical implications of AI are an important issue. As AI systems become more complex and autonomous, there is a need to address issues related to decision-making, fairness, transparency and accountability.

Data privacy and security are key considerations in AI. The collection and use of large amounts of personal data requires robust data protection and security measures to ensure trust in AI systems and the privacy of individuals.

The direction AI takes will depend on how it is developed, deployed and regulated. With responsible practices and proper guidance, AI has the potential to improve many aspects of life and address complex challenges.

However, open dialogue, collaboration and continual assessment of the impact of AI is needed to direct its development in ways that benefit humanity as a whole.

DO YOU BELIEVE ARTIFICIAL INTELLIGENCE MAY ADVANCE OR IMPEDE YOUR FIELD? HOW?

I believe that AI has the potential to advance and improve several fields of research, bringing faster and more accurate answers in several social sectors. AI technologies, such as advanced machine learning algorithms, natural language processing and deep learning, have already played a significant role in advancing the capabilities of models such as Alexa, Siri, Google and now ChatGPT. AI can help researchers and developers by automating tasks, providing insights and accelerating the pace of innovation. AI can also facilitate the development of new research tools and methodologies.

Additionally, as AI technologies advance, there is the possibility that systems will become more capable and potentially surpass certain tasks traditionally performed by human researchers.

In summary, AI has the potential to significantly advance the field of research and development, providing new tools, accelerating innovation and optimizing processes.

WHAT, IN YOUR OPINION, IS THE MOST IMPORTANT THING IN THE WORLD OF TECHNOLOGY?

In my opinion, the knowledge. But technology must serve and benefit humanity in social progress by bringing solutions, accessibility and promoting inclusion to all individuals, regardless of their abilities, socio-economic status or geographic location, and should strive to bridge the digital divide. That's all, folks!

Learn more about him at his personal website <https://wicasame.com/> and connect professionally on LinkedIn at <https://www.linkedin.com/in/wilsoncmendes/>

RANSOMWARE - ATTACKS ON THE RISE: ARE WE PREPARED FOR THE NEXT WAVE OF CYBERCRIME?

“New technologies create new opportunities for society, businesses, governments and criminals.”
Anonymous

The organization and industrialization of cybercrime are unmatched by any other crime. This evolution allowed would-be cybercriminals to continually improve their skills and profit opportunities. Similar to other criminal markets, such as narcotics, cybercrime is always looking for new opportunities to make profits and is also subject to demand and supply, the law that regulates any social segment.

The global emergence of Ransomware came at a time when stolen data was in abundance. The widespread adoption of new digital technologies has led companies to dynamically move from backward paper files to modern digital documents. The alluring promise of greater speed, dynamism, efficiency and profits has inspired governments and organizations to adopt new internet-based technologies to conduct business communications and transactions. This rapid adoption of technology has left many governments and organizations desperate as they are unprepared and unprotected for the types of cyber threats they would encounter.

This growing level of insecurity has left many companies and governments exposed, large volumes of sensitive data have been stolen, exposed and made available for purchase.

The beginning of any emerging market brings possibilities for lucrative returns, which allows a certainty to drive government regulators to intervene in an effort to restrict or prevent, and stamp down those that develop their natural flow.

This, for example, has already happened with gold, oil and even cryptocurrencies and other diverse assets, and today, similar concerns are being raised about big data. While tech giants such as; Amazon, Tik Tok, Microsoft, Google, Facebook and Instagram started planning how they could collect, analyze and monetize user data. Cybercriminals also developed new strategies to improve the scale and profitability of their online operations. Throughout the period of pandemic globalizations, governments, corporations, and society at large have rapidly adopted new technology-based systems, internet-enabled devices and other innovative ways to survive.



DATA FOR SALE: THE COMMODITIZATION OF PERSONAL INFORMATION IN A CONTROLLED SOCIETY

“Men are able to switch off their conscience as well as their electrical appliances, and sleep soundly.”

George Orwell - 1984

Data is generated and collected every second as information and communication become increasingly digital. These assets can be in the form of numbers, images, video, audio, or any type of data that can be digitized and used for a variety of purposes, from market analysis to preventing threats to cybersecurity. Groups that are able to collect and use this data accumulate power and influence. These groups can be businesses, government organizations, or even individuals.

The ability to collect and utilize massive amounts of data is one of the main reasons companies like Google, Facebook, Twitter, Tik Tok and LinkedIn have become so powerful. These companies have created data domains in the cyber world where they are able to collect and store huge amounts of information about their users. personally identifiable information such as names, addresses, dates of birth, financial information including demographics, interests, browsing history, purchase history, email address, behavioral information, and other personal information.

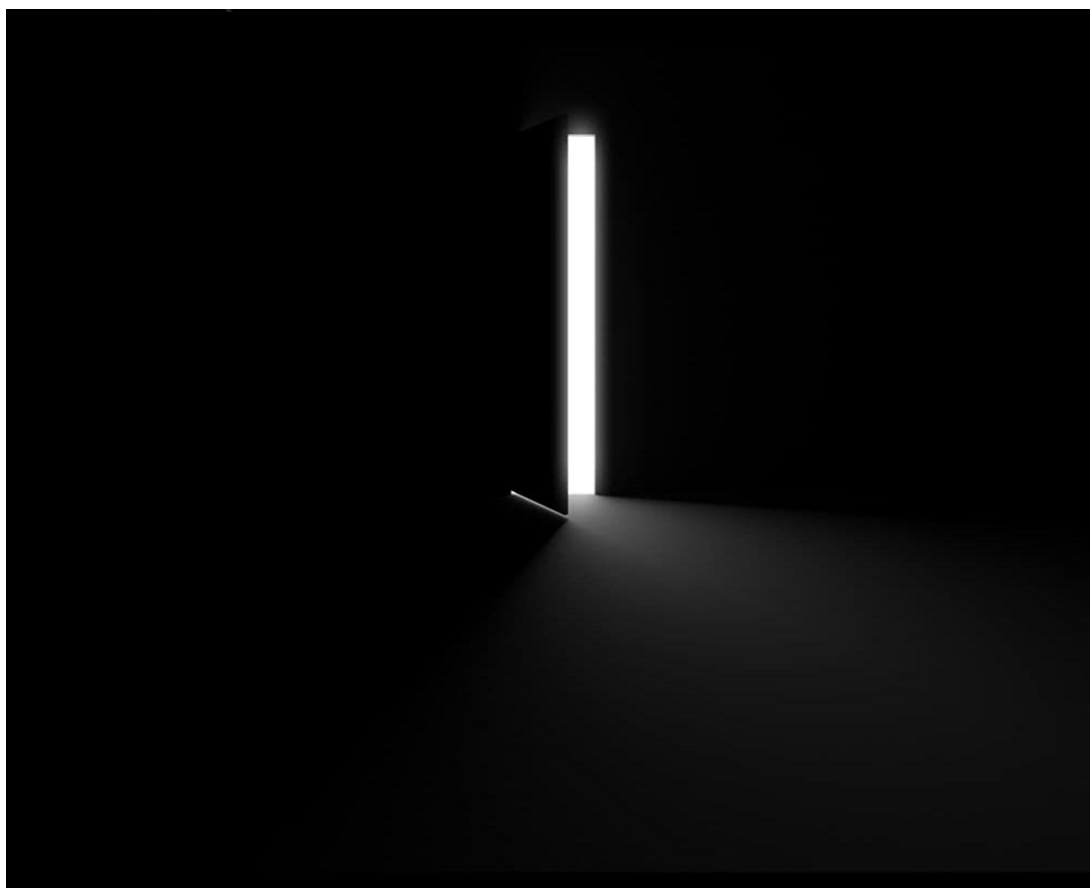
They use advanced techniques and complex data processing algorithms, such as big data analysis, to gain valuable insights and information that can be used to guide decisions and influence public opinion through the manipulation of search algorithms and recommendations. This raises concerns about user privacy and the commercialization of collected data with companies, governments, and organizations in general, which can provide valuable information and insights to help with decision-making.

In this article, we'll explore clusters of cybercrime-related data, how they operate, and how information security has become a critical concern for users.

Cybersecurity is an important concern for any organization that handles personal or sensitive data. Cybersecurity involves protecting systems, networks, and data from cyber threats such as malware, phishing, hacking, and other forms of cyber attack. Organizations must be prepared to deal with these threats and take steps to mitigate the impact of potential security breaches. Employees of these companies can be considered holders of privileged information about users, which represents a threat to the security of this data. They can access users' personal data without authorization and use it for personal or malicious purposes. They may also sell or leak this data to third parties, such as data brokers.



INSTAGRAM: THERE IS SOMEONE BEHIND THE DOOR



With the power of decentralized and distributed information, the data, containing rich and intimate information of the citizen, is increasingly accessible.

Social networks provide pentabytes of data from thousands of people around the world. Any public information produced from these networks becomes available and can be collected, explored and manipulated to an appropriate audience for the purpose of meeting specific ideals.

For the vast majority of people, user names, real names, social network, email, and phone numbers that can be directly linked to applications like WhatsApp, Telegram among others, real names and addresses, may not be dangerous. But...the results of these consultations can lead to indescribable places far beyond this vigorous article.

Instagram is a social network with photo sharing services, videos, geolocation, conversations and an impressive amount of data available with billions of connections between active users worldwide.

DANGEROUS IN THE AIR

AIRCRAACK-NG



“I was at agenda 2000 and one of the people who was there was Craig Mundy who is some kind of mucky muck at Microsoft, I think vice president of consumer or something like that and I hadn’t actually met him. I bumped into him in an elevator and I looked at his badge and said:

- I see you work for Microsoft
and he looked back at me said:
- Oh yeah! and what do you do?

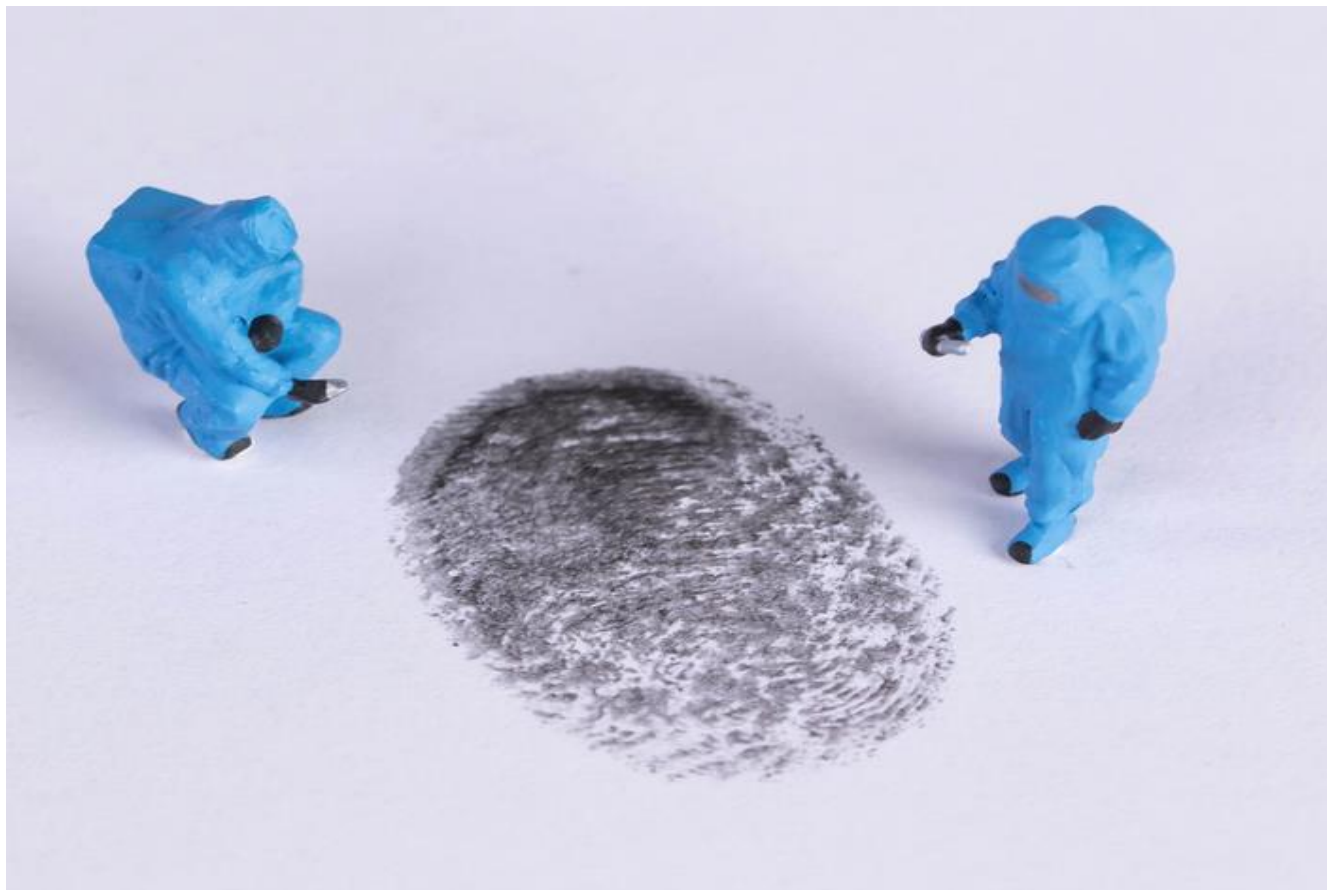
And I thought he seemed just sort of a tad dismissive - I mean here’s the archetype well you know guy in a suit looking at a scruffy hacker and so I gave him the thousand-yard stare and said:

‘I’m your worst nightmare.’

Eric Raymond – Revolution OS

The invention of microprocessors, from wristwatches together with the deluge of hardware hitting the market, development of the Raspberry Pi, Chromebook, CubieBoard, BeagleBone ARM-based computers, for example, made it possible to access increasingly affordable devices, thus creating a new, empowered and creative society of ordinary people.

FORENSIC INVESTIGATOR MOBILE IN THE LOST WORLD OF CRIME



“Alice asked: Can Cheshire Cat tell me which way I should go? That depends a lot on where you want to go, said the Cat. I don't know where to go! said Alice. If you don't know where to go, any road will do.”
Alice in Wonderland

Today's smartphones are much more used for socializing than making phone calls. Tablets, increasingly equipped with powerful processors and much more storage capacity, are no longer used only as entertainment devices. Smartphones and tablets are replacing camcorders, digital cameras, book and newspaper readers, TVs, navigation and communication devices, and even game consoles, competing very successfully for users' attention with computers and smartphones.

With this amount of time spent on mobile devices and the vast array of activities available on them, smartphones and tablets have become great digital storage vaults for personal and professional secrets, providing a veritable wealth of information about their users.

Extracting this information, analyzing the data and turning it into solid evidence is the main objective of a digital investigator and for that the examiner may need to break these encryption mechanisms to extract data from the devices. For any collection of evidence that does not follow the proper procedure during the examination may result in loss or damage of the evidence and render it invalid in a legal process.

CATCH ME IF YOU CAN

"The cat was once seen, sitting on a roof, indoctrinating some sparrows perched just beyond his reach. He told them that all animals were comrades, and any sparrow he desired could land on his hand; but the sparrows preferred to stay away." Animal Farm - George Orwell

INTRODUCTION

With this exponential growth in the digital universe, mobile devices and connections that includes valuable information, and are becoming a huge repository of confidential data becoming more and more powerful as personal computers, started to be part of the routine of people all over the world, surpassing the world population and adding up to more than 8 billion devices.



Along with this advancement, and using the same technologies, given the pace at which mobile development is progressing, everyday tasks, such as sending and receiving emails, sharing photos and videos, accessing social networks, banking, managing tasks and reminders, are part of our routine. Because of this advancement, every day the world's media reports cases involving eyewitness computers, cell phones, IoT, vehicular systems, drones, smart watch, wearables tablets and cloud storage.

It is no surprise that governments, phreaking, spy agencies and criminals, due to the ease of access to citizen data and technological manipulation, began to gain advantage by using evidence and social involvement to facilitate their crimes.

THERE IS HONOR AMONG THIEVES

The rapid technological development and the potential access by companies and users during the period of the pandemic brought with it a significant, uncontrollable and much more complex increase in cyber crimes, leading to the simultaneous compromise of thousands of computers, tablets, watches, smartphones, refrigerators, automobiles and a series of IoT devices, directly targeting different types of operating systems, such as Windows, Unix, iOS, Mac, Linux, and Android.



To stay optimally organized, corporate and personal data is stored on these devices, containing scientific research, valuable operations and trade secrets, financial information and military strategy, characteristic of corporate environments and government institutes. Making people increasingly trust their devices, fixed or mobile, significantly increases dependence on digital technology.

To always stay one step ahead of defenders, cybercriminals use anonymization networks, such as the Onion Router TOR network and/or i2p, to communicate. These networks have large and diverse attack surfaces, containing domain addresses that are always resolving new host IPs, allowing cybercriminals to move around the Internet with relative security by supporting activities such as:

- Hosting emails/phishing – By creating fraudulent emails sent without the recipient's permission to promote matters of interest to the victim, usually captured through social engineering, on networks such as LinkedIn, Instagram, Twitter, Facebook... Cyber criminals use the names and logos of organizations known to these followers, selected through these social networks.
- Anonymous websites – Containing real-time chat and file sharing, creation of hundreds of thousands of info, org, click and ru domains, for example, and IP addresses that change very quickly, protecting

communications from surveillance and monitoring by governments, providers, agents and so on. This makes it even more difficult to track the exact location of criminals, creating ample possibilities for attackers to infiltrate using hundreds of modern tactics.

Cyber criminals can abuse services like these to spread malware, meaning that a successful attack against uninformed people and an unprotected system can have catastrophic consequences. In practice, these are the main targets of cybercriminals.

There are now, due to these changes and disruption in the information age, several types of cyber crimes, and one of the most feared, popularly known as digital extortion or digital blackmail, is ransomware.

Ransomware is an intelligent and mutating species of malicious software, with hundreds of codes available on github, which normally prevents companies, governments and users from accessing their devices and personal data through some encryption method, demanding payment for the release of the data, with redemption through cryptocurrencies like Bitcoin and Monero, for example.

There are several ways of distributing this malware; ransomware can come together with other software programs, associated with a .dll file or executables, such as keygens, crack, patch updates, files downloaded from unknown sources via Torrent containing attachments in .pdf, .doc, movies, music or some kind of .png or jpeg file, or it can come through malicious pop-up ads or the automatic download of ransomware as soon as the user loads the page in a browser where the malicious ad is hosted, features of pornographic sites.

Ransomware mutations often install and utilize complex systems using the TOR network as a secure communication channel with their command and control servers being updated, on average, every 30 minutes (<https://www.dan.me.uk/tornodes>) giving the attacks even more popularity.

Malicious advertising, Spear phishing, Landing page, Malvertising, Viruses, worms Ransomware. Cryptojacking, Scareware, Spyware, Trojans, Rootkits, Botnet, Keylogger ... These are forms of attacks through these advanced techniques.

There is a constant stream of custom attacks on an organization, individual or company to steal and hijack information using exploits that exploit vulnerabilities in even protected systems, yet containing antivirus solutions are not enough to prevent a ransomware attack that is widely capable of disabling a network, leading in most cases to compromise the data on the victim's computer or the device becomes unusable until the device owner pays the ransom, without any kind of guarantee that their files will be released, to remove the restriction.

It is estimated that there are more than 682 million victims, increasing each year, worldwide. The longer an infected system runs, the more difficult it will be to recover these files directly from the hard drive.

FORENSIC TOOLS?

ELEMENTARY, MY DEAR WATSON

“Writing is 1% inspiration and 99% elimination.” Louise Brooks

Introduction

Currently, with the increasingly present amount of data hosted in clouds, through systems and applications, information technology, driven by the easy access to billions of leaked user data, also becomes attractive to a multibillion-dollar global industry of fraud, theft, kidnappings, blackmail, fake news and so on. Reaching all criminal fields, it becomes more and more part of almost everything around us.

Operating systems, applications, mobile operators and internet access providers track a significant amount of information about the actions that a user takes.

Instagram, Uber, Facebook, Tinder and hundreds of other apps have access to your contacts, location, microphone, video camera, device ID, text, audio and video conversations, wifi networks and a multitude of metadata.

Google, for example, tracks geolocation information, contacts, search history, email, downloads, calendar, play store, browser activities, who the user communicates with, payments and what they buy.

Data leakage remains one of the major problems in today's tech world. To analyze modern crime, you don't need magnifying glasses or hire the legendary Sherlock Holmes.



HOW TO MAKE CYBERSPACE SAFE

In mathematics, the shortest path between two points is a straight line.
In technology, the shortest path between two points is the click.

The Internet has a very low barrier to entry and is constantly changing every day, unlike atoms, which rely on customs for surveillance, monitoring and border controls, the powerful and complex bits of data through computers, smartphones, tablets, watches, smart TVs and IoT devices, circulate freely across continents, making everyone reach each other.

With the pandemic, the role of the Internet has become very active and dominant, being part of the modern lifestyle and bringing a notable impact on people's lives, allowing several ruptures, creating a totally new environment.

As the Internet has overcome traditional media, time limits and geographic boundaries, it has become a central medium for information exchange and communication. Certainly, business models were disrupted as new business models were created, with this advancement, its impact can be witnessed in all spheres of society around the world. The intense and continuous use has made the transfer of information faster and more efficient, making the internet a much more powerful and complex system than any of us can understand.

With this growth, added to billions of data leaked on the internet, together with personal information spread on social networks such as Instagram and LinkedIn, for example, social engineering and different types of malicious attacks are increasingly present and sophisticated in the user's day, taking advantage of available personal information to apply various scams, often using this exposed user as a means of transport to reach companies and organizations, causing the exploitation of security related to Internet systems and its services.

These attacks use a mixture of techniques and tools as true technological weapons, such as denial of service attack, spam, phishing, push, social engineering, polling, etc. They cause economic losses to companies and have a very bad impact on business, security, and network infrastructure.

As new hardware and software features are developed and new protocols are implemented, network security has become predominant in the market, as traditional defense models have not been sufficient to predict and protect web servers, email servers and network servers from attacks and hijackings.

In this environment, a new field is emerging and rapidly evolving in the face of so many incidents that devastate traditional security resources compromising confidentiality and integrity, making many services unavailable.

MALWARE - THE NIGHTMARE TIME

Introduction

The evolution of technology and the rapid growth of the internet have brought the threat of cyber attacks to private and public infrastructure.

Words like backdoors, spyware, worm, keylogger, trojan, miners, botnet, rootkit, and ransomware

With the arrival of the Internet of Things, we have many more devices available, significantly increasing connections to access information; watches, refrigerators, lamps, smart homes, smart TVs and various devices that are already part of our daily lives, bringing great changes to our lives, increasing the ability of cybercriminals to act. This has revolutionized the way organizations do business.

Governments, the financial sector, the public sector, large corporations, electric and energy companies, the data centers of hundreds of segments around the world are at this very moment compromised.



A data breach is more and more common in our lives, it is not difficult to find a lot of information about the company, about you, about me, about us. In the internet space, we have a very big opportunity to get a credential.

Data centers in hundreds of social segments around the world are currently compromised through security breaches.

STEGANOGRAPHY – PROTECT YOUR DATA

“A picture is worth a thousand words.”

Fred R. Barnard.

Will be?
What do you see?

Inside this image there is the possibility of inserting: audios, videos, texts, trackers...and a lot of information. Steganography is a technique of hiding information with a secret message in something that is not secret, decreasing the possibility of suspicious detection during data communication.



In the age of digital technology, data brokers and insecure networks communication, we have a lot of apps and social networks that use the Internet to transmit and store large amounts of data.

To keep authorized persons away from spies, hackers, governments and new threats against the transmitted information, a variety of techniques have been introduced; encryption and steganography are two of them. To help explain the difference between encryption and steganography, encryption hides the meaning of the message, steganography hides the existence of the message. Encryption is beyond the scope of this article.

USA vs Eddie Gallagher

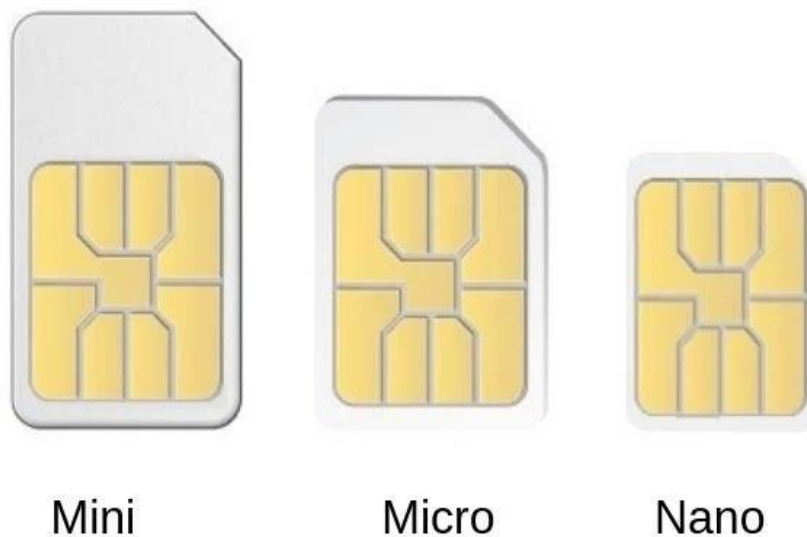
In a famous case that became known worldwide, USA v. Eddie Gallagher, investigating the Special Operations Chief Edward Gallagher on war crimes charges including murder, in April 2019, attorney Marc Musakasey emails the case's chief prosecutor, Chris Czaplak, notifying him that he had joined the defense team. Three seconds later, he receives an email back from the chief prosecutor welcoming the case.

MOBILE SERVICE BREACH - BEHIND THE SCENES WORK

Phreak - "A person who is obsessively interested in learning about, exploring, making free calls and playing with the telephone network."

Starting

Almost all mobile phones need a subscriber identification module, better known as the popular SIM card, before they can be enabled. The SIM contains an integrated circuit and memory to store SMS messages and contacts, it also authenticates the phone, helps locate it in a network and is responsible for identifying the phone with the operator so that calls and data can be forwarded to other phones and devices



Mini

Micro

Nano

Warning

All information available in these articles are for educational purposes only. Use them at your discretion, the author of the article and the owners of eForensics magazine cannot be held responsible for any damage caused. The opinions expressed in this article are our own and do not necessarily reflect those of our employers. If you don't know how to attack, you won't know how to defend. The author of the article and eForensics Magazine are not responsible for any damages or failures attributed to said article.

ABOUT THE AUTHOR

Wilson Mendes - Cyber Security Consultant | Penetration Tester | Red Team | Writer

<http://www.wicasame.com/>

<https://www.linkedin.com/in/wilsoncsmendes/>

Cyber security and Pentest Red Team professional with over 22 years of experience in Information Technology. Specialized in cybersecurity, with proven expertise in penetration testing, advanced encryption, security protocols, malware, identifying vulnerabilities and strengthening defenses against cyber-attacks. My skills range from analyzing cybercrime, implementing robust firewalls, and administering Linux and BSD networks, ensuring effective security measures. Familiar with information security standards such as ISO/IEC 27001, ISO 27002, ISO 22301, NIST, GDPR, LGPD, HIPAA, PCI DSS, SOC, ITIL, FISMA. Committed to protecting valuable assets and providing effective solutions.

An active author, I write technical articles for the renowned magazines eForensics Magazine and Hakin9, actively contributing to the cybersecurity community. Ready to face complex challenges and contribute to safe and reliable digital environments, I have organizational and interpersonal skills that allow me to work in global environments.



BECOME A DEEPPFAKE AUDIO MASTER

DEEPPFAKE AUDIO: A COMPREHENSIVE
STUDY IN DIGITAL FORENSICS

Raahat Devender Singh



THE WAY AUDIO ENRICHES OUR UNDERSTANDING OF THE WORLD AND SHAPES WHAT WE PERCEIVE TO BE THE “OBJECTIVE REALITY” OF THINGS HAS ONLY GROWN TO BE MORE PROFOUND AND IMPLICIT.

Join Us!

eForensics

magazine & courses

ONLINE COURSES



MICRO-DRONE WARFARE
CYBERSECURITY IMPLICATIONS AND COUNTERMEASURES

Rhonda Johnson

The cover for the course 'Micro-Drone Warfare' features a dark, atmospheric scene with a person in a hooded jacket in the foreground, looking towards a bright, fiery sky where several small drones are flying. The overall color palette is dominated by dark blues, greys, and oranges from the fire.

EFORENSICS FOR EWARFARE

Dauda Sule

The cover for the course 'Eforensics for Ewarfare' depicts a high-tech control room or operations center. Multiple computer monitors are visible, displaying various data visualizations, maps, and charts. The room is dimly lit, with light coming from the screens and overhead fixtures, creating a professional and technical atmosphere.