Conciencia Digital
www.concienciadigital.org

ISSN: 2600-5859
Vol. 3, N°2.2, p. 80-96, junio, 2020

Electronic methods for obtaining IP addresses through webmail and social networks

Métodos electrónicos para obtención de direcciones IP a través de webmail y redes sociales

Gabriel Vinicio Moreano Sánchez. [1], Edgar Vinicio Ávalos Yuque . [2], Victor Hugo Benitez Bravo. [3] & Alvaro Gabriel Benitez Bravo. [4]

Recibido: 12-02-2020 / Revisado: 05-03-2020 /Aceptado: 12-04-2020/ Publicado: 05-06-2020

Abstract.

DOI: https://doi.org/10.33262/concienciadigital.v3i2.2.1247

Obtaining data is a fundamental stage in a computer security process both to identify violators or to detect vulnerabilities in a certain system. For tasks such as investigation or intelligence, among the most important information that can be collected from an entity are the IP addresses of important people, suspects or investigation targets. Obtaining this information for legal and ethical purposes is currently more complex because service providers mask this data in order to protect the identity of their users. In order to obtain the IP address, it is intended to apply different electronic and automated techniques that serve to modify documents and cover them up so that, when opened by the recipient, they reveal their IP address, which will be automatically registered in the logs of the web server that is implemented in this research. These approaches will be considered: sending an invitation HTTP link directly and sending an Office document with invisible characters. The scope of the work described is important, since it covers proposed techniques for detecting an IP address using various methods evaluating the efficiency and effectiveness of each test. This will allow the forensic analyst or investigator to obtain a person's possible location by consulting with internet providers.

Keywords: DNS, IP Address, Webmail, Social Networks, Forensic Analyst.

[1] ESPOCH, CIMANT, Riobamba, Ecuador, gabriel.moreano@espoch.edu.ec, ORCID: https://orcid.org/0000-0002-9331-8223
[2] Telefónica, Quito, Ecuador, vinycioavalos@hotmail.com, ORCID: https://orcid.org/0000-0001-7458-9370
[3] Universidad Tecnológica Israel, Quito, Ecuador, vhbenitez@uisrael.edu.ec, ORCID: https://orcid.org/0000-0002-8975-3644
[4] Universidad Tecnológica Israel, Quito, Ecuador, agbenitez@uisrael.edu.ec, ORCID: https://orcid.org/0000-0002-8465-1059

ISSN: 2600-5859
Vol. 3, N°2.2, p. 80-96, junio, 2020

Resumen.
La obtención de datos es una etapa fundamental en un proceso de seguridad informática tanto para identificar infractores o para detectar vulnerabilidades en un determinado sistema. Para tareas como investigación o inteligencia, entre la infor-mación más importante que se puede levantar de un ente están las direcciones IP de personas importantes, sospechosas u objetivos de investigación. Obtener esta información con fines legales y éticos, actualmente es más complejo debido a que los proveedores de servicios enmascaran este dato a fin de proteger la identidad de sus usuarios. Para obtener la dirección IP se pretende aplicar diferentes técnicas electrónicas y automatizadas que sirvan para modificar documentos y encubrirlos de modo que, al ser abiertos por el destinatario, nos revelen su dirección IP, la cual quedará registrada automáticamente en los logs del servidor web que se implementa en esta investigación. Se tomará en cuenta estos enfoques: el enviar directamente un enlace HTTP de invitación y enviar un documento de Office con caracteres invisibles. El ámbito de aplicación del trabajo descrito es importante, pues abarca técnicas propuestas para la detección de una dirección IP mediante varios métodos evaluando la eficiencia y efectividad de cada prueba. Esto permitirá al analista forense o investigador, obtener la ubicación posible de una persona al consultarla con los proveedores de internet.

Palabras claves: DNS, Dirección IP, Webmail, Redes sociales, Analista Forense.

Introducción.

In modern times the advancement of technology is exponential. Everything changes minute by minute, and this has generated great advances and changes in society such as more agile markets, online education at all types of levels and borders, more continuous communication with our loved ones and others, but it has also caused new problems such as: crime, alteration of public and private information, falsification of documents, large-scale scams, disappearance of bank accounts, etc. In this work we focus on the merciless attacks on cyber media that cause a global scandal by revealing private or confidential information, a situation that no one is except for. We are witnesses to the birth of viruses, malwares that attack the computer systems of the world causing irreparable damage to storage infrastructure, file integrity in a company or other computer users.

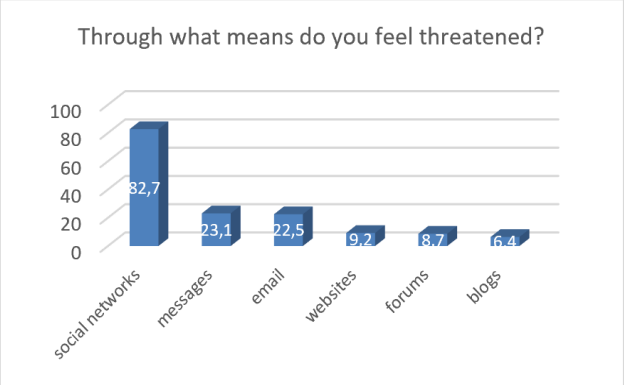
This insecurity has resulted in new social ills and the enlargement of others that already exist, such as: cyberbullying, child pornography, child trafficking, drug trafficking, etc. In this work the ways of detecting the person or persons located on the other side of the computer or mobile device are considered; Identify them so that justice can proceed against them. In Latin America, several surveys indicate that social networks are the main route of harassment, that is, traditional harassment has migrated towards information and communication technologies and especially social networks.

According to the company Eset - Latin America, an informatics security company, in 2013, cyberbullying showed the following statistics: 30.7% of adolescents in the region aged 12 - 20

ISSN: 2600-5859
Vol. 3, N°2.2, p. 80-96, junio, 2020

were victims of Internet harassment. The main route of these attacks was social network like Facebook, Twitter and Google Plus with 82.7%.

Figure 1. Ways of harassment



Prepared by: Research Group.

In (De Juventud & De, 2017) the impact of bullying and cyberbullying is widely shown, in a doctoral thesis (Gonzales García, 2015) the author shows us an approach to antisocial behavior in cyberspace and how this generates a high risk over the most innocent people and also shows us certain strategies to counteract this problem. In (García Maldonado, Joffre - Velásquez, Jesús Martínez - Salazar, & Llanes - Castillo, 2011, Ximhai, 2014) we find a specific summary on how this problem affects the most exposed people who are adolescents and children, finally (Herrera - López, Romera, Ortega - Ruiz, & Ortega - Ruiz, 1996) give us a vision about the impact of this type of unethical harassment in our region.

In Ecuador since 2014, date on which the Comprehensive Organic Criminal Code (COIP) came into force, cybercrime is considered and sanctioned, and which is committed through the use of computers, communication computerized devices or an informatics system.

According to the National Police of Ecuador "in the country, 85% of computer crimes occur due to carelessness of users when accessing social networks, using smartphones, email or using passwords, this is gives false advertising posts or malicious emails requesting password changes and others. Also, excessively exposing information on social networks such as Facebook, Twitter, Instagram and others facilitate the work of scammers, extortionists, kidnappers, and those who are involved with child pornography, "the excess information on the networks causes much People have access to that information and that may violate emails, bank accounts and others by skipping security questions with dates, names, studies or jobs of the victim. From January to May 2016, 530 complaints for computer crimes were presented to the Ecuadorian State Attorney General's Office, the majority corresponding to fraudulent appropriation by electronic means. (Arroyo J. Richard, 2016). The computer crimes that occur most frequently in Ecuador are electronic fraud and child pornography; For this reason, this research is proposed in order to mitigate this problem.

ISSN: 2600-5859
Vol. 3, N°2.2, p. 80-96, junio, 2020

At an industrial level, it is also important to show a high level of safety in order to protect valuable data and information, in (Oscar Fernando Castellanos, Montañez, & Fonseca, 2007) a summary on how digital marketing and a virtual model strengthens the industry was identified. In (Sarmiento, Guerrero, & Argote, 2016), basic parameters of safety within Wi-Fi are described, which makes it difficult to obtain certain information such as the IP address, in (Martínez, Caicedo, Hernández, Caicedo & Hurtado, 2007) another method of computer security focused on virtual commerce is described. While (Arndt & Actis, 1996) and (Robert T. Baum, 2003) show patents specialized in protecting information which detects possible cloning in IP addresses.

PYME's are also the target of these digital criminals and specifically attack the servers of these entities in an effort to violate their banking systems and obtain information from their clients to assign them as new victims, in (Johanna Martínez Molina et al., 2009) the authors propose a double firewall filtering technique to avoid these attacks on servers, a system that will help stop certain attacks but will not release information from those responsible.

To improve security systems in all areas of society, residential, commercial and industrial areas, processes for verifying security levels have been developed, that is, there are companies that are dedicated to commercializing services in computer breaches in order to to find errors in the systems and correct them, and there are other types of companies that are in charge of certifying security levels, in (Bracho et al., 2017) a form of computer audit is presented according to the OSSTMMv3 methodology, a very respectable approach to verify the security of certain computer systems, while (Ibarra & Electrónico, 2004) presents a general approach to how technology auditing helps public and private companies and legal and natural persons to maintain an adequate level of digital security, from Likewise, conductive rules for the use of computer tools are shown in order to keep our information safe.

This work focuses on obtaining information from cyber attackers not necessarily after they have carried out a wrongdoing, but rather obtaining information from people who are presumably digital criminals, specifically seeking to obtain their physical location by identifying the IP address from where If fraudulent operations are taking place, the automated identification process attacks the target with various automated digital tools in order to mislead the target and succeed in the task.

Methodology

In order to carry out the experiment, we worked on the installation and configuration of a web server to store the logs of people, where through social engineering and by clicking on a link, when opening an office document, those become the object of this investigation.

Web Server Configuration

For the present investigation the Microsoft Azure cloud platform is manipulated, along with the operating system as a virtual Windows Server 2016, with internet information Server (IIS). The configuration of the web server is carried out under the following considerations: basic

ISSN: 2600-5859
Vol. 3, N°2.2, p. 80-96, junio, 2020

configuration name WS2016, HDD virtual machine disk type, user name and password. To install the server we considered a near place to Ecuador and the other fields by default. The size of the virtual machine is allocated two cores, RAM of 7 GB, 14 GB of disk storage. The most important step in this configuration is: the network settings where NAT is configured to port 80, to make the web server accessible from all over the world.

Once the virtual machine was created, you can see its structure, with buttons to connect, start, restart, stop among other options similar to those found at the desktop virtualization tools. A remote connection is used to connect to the virtual operating system. The connection to Microsoft Server 2016 Datacenter is through a remote desktop. When the configuration is done, a file is downloaded, which is double-clicked to enter the credentials. The web server is configured with the IIS installation manager, with the minimum requirements being used in this investigation. When entering the public IP assigned by the Microsoft Azure platform in a browser of the web server or any browser available in any location: the initial page of the web server is loaded.

Web Bug

In informatics, a Web Bug is considered as a web beacon or a tracker, an invisible image to the human eye with a size no larger than / x / pixels; but that can be inserted on a web page or in an e-mail message. It is used in order to control whether a person has read an e-mail or visited a web page (ideal for the marketing of a company). This allows a control of views of a specific page, as well as various functions such as web analysis. The Web Bug designed for this research will recover the public IP of visitors to the web page configured for this study.

Web Page

A new interface is customized creating a web page with the name "TFM MSI". Therefore, we proceed with the verification by entering the public IP address 192.232.34.208; It also adds the Web Bug that will serve as a tracker. In the same way, in the testing stage, the address of the image is sent by social networks or by email using social engineering.

Web server Logs

Under the observation of what IP addresses were opened the image or Web bug, with url **http: //191.232.34.208/images/virus.jpg**, stored in the web server; it is necessary to watch the folder logs **C:/inetpub/logs/logfiles/W3SVC2**, where it is shown the year, month, day, exact time, archive name, used port, and most importantly, The public IP address of the device which is important to stress on the folder´s name **/virus.jpg** just to set an example of this research. This points out precisely that such folder may hold malicious programs in a real environment the archives names that have been used should not raise any suspicions.

In order to acquire the reports in real time, the power shell tool is used from Windows server 2016 Datacenter; under the following command **c:/inetpub/logs/LogFiles/W3SVC2> Get-content./filename.log-Wait.**

ISSN: 2600-5859
Vol. 3, N°2.2, p. 80-96, junio, 2020

Word 2016 Document Configuration

For the next experimentation, the Word 2016 version is used, with the option of quick elements. Choosing and inserting a field named "**Include picture"** referencing an image stored on the web server. It is important to emphasize that, by means of this technique, the complete image is not inserted in the document, but only a link to it. In such a way that the document to be opened, the system will connect to the web server, in order to load the image and be able to show it. In this way, we make sure to get a trace of the object each time you open the document.

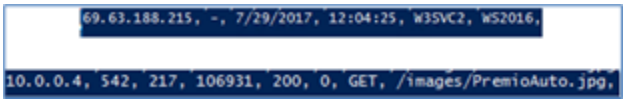
IncludePicture Field

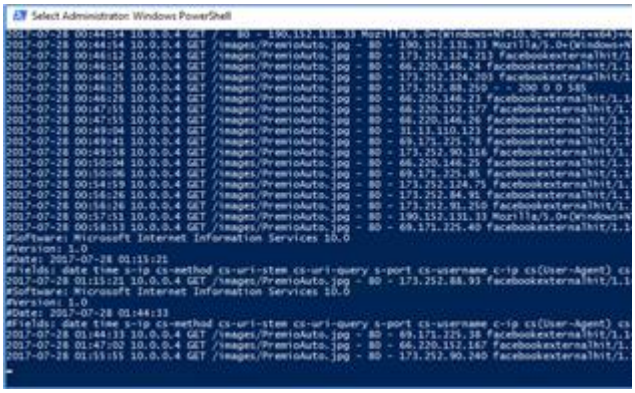
The referenced address is **http://191.232.34.208/images/virus.jpg**. Note that this test works with any version of Word installed on any operating system. This test is done by attaching the file to an email to send it later to the target, person or target, to perform the operation we enter text in the document, for later send it to the target. As you can see, the Web Bug appears before the text. Although in this case, we have used a black dot in order to make it visible in the tests. In a real case, a transparent or white pixel would be used, so that it would not be visible to the user, but it would still have the same effect.

Results

Graphic 1. localizer IP

ISSN: 2600-5859
Vol. 3, N°2.2, p. 80-96, junio, 2020





ISSN: 2600-5859
Vol. 3, N°2.2, p. 80-96, junio, 2020

Prepared by: Research Group.

Test son Social Network Facebook

Sending the URL to the target. It is used for this test in a web page stored in Windows Server 20016 Datacenter on the Microsoft Azure cloud. The Web Bug is configured in size 1x1, the URL contains the Web Bug to be sent to the target. For these tests, shipments are made between two accounts: the one that will send the messages created expressly for this purpose, and the one that will receive the messages, which is the account of the objective of the investigation. The Web Bug is included as a tracker **http://191.232.34.208/images/PremioAuo.jpg**. A fake Facebook account with random data is then configured. As next step by remote desktop, you enter the server to modify the file **index.html** with the web Bug.

Figure 2. Web Bug draw

Prepared by: Research Group.

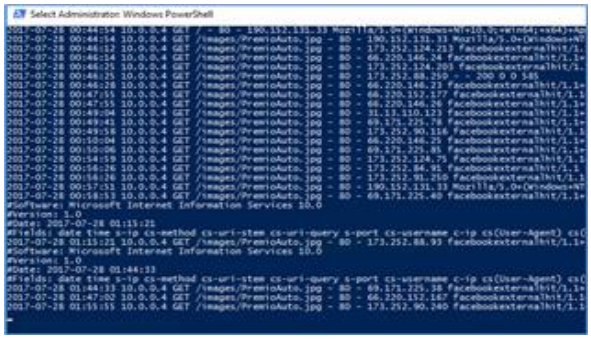
Test 1. Facebook share a publication

To check this method, a publication is created with the link **http://191.232.34.208/images/PremioAuo.jpg**, which shows the draw of a car that will be made soon, the objective of this test is to prove the scenario, check if the method proposed is valid and analyze the results obtained by the people who entered the website that contains the Web Bug. Prior to the publication of this publication in the created account, it is added to as many people as

ISSN: 2600-5859
Vol. 3, N°2.2, p. 80-96, junio, 2020

possible, obtaining in a few hours a large number of accepted friend requests. The Logs shown in Figure 3 indicate the entry to the page with the tracker, the high interaction with only seconds of difference stands out in this test.

Figure 3. Logs test auto raffle



Prepared by: Research Group.

In the same way, it is appreciated that the income is made from several IP addresses, these addresses correspond to Facebook data centers and do not correspond to those of the users as shown in Figure 4 when reviewing the WHOIS records with the address **173.252.124.21**. therefore, we can conclude that this is not a valid method to obtain the IP address of our objective since the connection to our web server is carried out by the Facebook systems themselves, which in turn will later serve this content to the recipient. In short, by this method, we do not obtain an IP address that identifies the target.

Figure 4. WHOIS Records

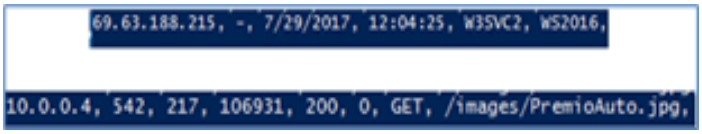
Prepared by: Research Group.

Test 2. Facebook send URL private message

For the next test the individual sending of the URL is done by direct message. Obviously, in a real case it would be necessary to carry out a study of the objective in order to elaborate a publication adjusted to its interests, in order to obtain greater efficiency.

ISSN: 2600-5859
Vol. 3, N°2.2, p. 80-96, junio, 2020

Figure 5. Web server logs direct message



Prepared by: Research Group.1

The target is identified, and the URL is sent by private message. It is appreciated that the target has seen the message at **12:04**, to determine the IP address, it is necessary to go to the Server Logs (fig 5), thus verifying that the time is the same as registered by the social network when opening the attached link and IP address **69.63.188.215.**

Figure 6. Localización IP mensaje directo

Prepared by: Research Group.

Continuing with the development of the test, the discovered address is entered in a geo locator of IP addresses showing the information of Figure 6.

The data obtained do not correspond to the possible location of the objective based on the study carried out, as the Internet service provider or ISP indicates that it is Facebook, in these cases the location is questionable, as shown in figure 7 when geo is localized the same IP address **69.63.188.215.**

ISSN: 2600-5859
Vol. 3, N°2.2, p. 80-96, junio, 2020

Figure 7. Wrong location IP address

Prepared by: Research Group.

With this experimentation it is concluded that the IP addresses found correspond to the Facebook servers which download the photograph and these are registered in the Logs, once again these IP addresses do not correspond directly to the users who opened the link, and therefore he deduces that this method is not valid.

Tests with Webmails

In this section tests are carried out with Webmails sending emails between Gmail and Outlook accounts, for this purpose it uses URLs that reference images or Web Bugs, in addition to a file to capture the Logs and later georeference IP addresses.

Test 1. URL directly linking

The first test is to reference the URL with the Web Bug **http://191.232.34.208/images/PremioAuto.jpg** in an email message in Gmail and send it to another Outlook email account. Use the option to upload photos then add the URL, by pressing the button insert the image will be referenced, to better convince the target or person who receives the mail in the subject field can be placed a legend, after this the sending is made. When opening the email in Outlook, it is observed that the message has arrived at **18:39.**

In the logs of the web server, the address 191.232.34.208 can be seen, that is, the place where the email was opened.

Figure 8. Test 1 Log when opening mail in Outlook

Prepared by: Research Group.

By georeferencing the IP shows the location of the web server that opened (Figure 9) the mail however the information is not conclusive, they are Microsoft machines that download the image,

ISSN: 2600-5859
Vol. 3, N°2.2, p. 80-96, junio, 2020

and serve the recipient. There is no contact between the target and the server, so this test is not valid.

Figure 9. Mail opening location

Prepared by: Research Group.

Test 2. Attaching Word Document

This test consists of sending a name attachment **test 2tfm.doc** between email accounts Gmail, the previously configured document contains a WEB Bug in the address ***http://191.232.34.208/images/virus.jpg*** referencing the Web server to register logs when opened. It also includes the URL ***http://191.232.34.208/images/PremioAuto.jpg*** in the email message that just like the previous link contains a Web Bug which will allow you to determine what time the mail was opened in the registered Logs.

The sent is done from the account **vinycioavalos@gmail.com** to the post office **3hchocoatl@gmail.com**. mail opens **3hcho-coatl@gmail.com** and the message is appreciated.

It analyzes the logs (Figure 10) and determine interaction with the address PI **186.46.255.168** with hour 20:30:09 indicating that the attachment was read.

Figure 10. Test 2, logs URL and attached file

Prepared by: Research Group.

The hit of the logs, which gives us the IP of the target corresponds to the document of Word and the URL ***http://191.232.34.208/images/virus.jpg.*** In addition, it draws attention that, in this case, unlike the previous one, in which the target account was @outlook.com, the target computer also directly accesses the image we have linked by URL. When consulting the referential location (Figure 11) of the address IP and possible place where the mail was opened, it can determine the Internet provider CNT.

ISSN: 2600-5859
Vol. 3, N°2.2, p. 80-96, junio, 2020

Figure 11. Test 2, Referential location

Prepared by: Research Group.

To deepen the study of the original message of the received mail, just download the file **"txt"** that contain the technical headers, for example:

"Delivered-To: 3hchocoatl@gmail.com
Received: by 10.176.17.71 with SMTP id g7csp2940615uac;
Sun, 30 Jul 2017 17:48:00 -0700 (PDT)
X-Received: by 10.237.36.38 with SMTP id r35mr21284604qtc.327.1501462080165;
Sun, 30 Jul 2017 17:48:00 -0700 (PDT)"

Tests in Tor networks

The URL **http:// 191.232.34.208** it will be executed from the anonymous browser to later proceed to an analysis of the logs. As a final test of this investigation, the test will be done in TOR, opening the URL in the browser. The records obtained by the visit of the website are those shown in Figure 12:

Figure 12. Logs TOR

Prepared by: Research Group.

A direction is detected IP but it is not the same when performing tests on different pages, the location is not reliable and the IPS is in another country despite that in the test and experiments carried out from known locations.

Figure 13. Wrong location in networks

Prepared by: Research Group.

ISSN: 2600-5859
Vol. 3, N°2.2, p. 80-96, junio, 2020

Conclusions.

- In the present investigation, different methods have been tried to obtain directions IP of a user in social networks and Webmails. Using the facebook social network, if you try to link an image through your URL through different forms (publication on the wall, direct message; etc.) emphasizes in particular that the locations of the IP addresses found correspond to servers or data centers of Facebook. This address does not belong to the users directly and therefore, this is not a valid method to obtain the IP address of an objective. The same happens when performing these tests with webmails, If we try to embed in the message an image referencing it by its URL.
- Finally, it has been possible to verify that the technique of embedding the image in a document of Word (using the field code Include Picture), If it is effective for the target pursued, because once that file is made to the recipient, Target pursued we will obtain a record of your address IP, as well as other data revealed by the field User-Agent, such as the operating system and software used. However, it should be recalled that the identify an IP address published where it comes from a message, it does not guarantee the immediate location of a person; because this network can have multiple devices that connect to that address: therefore, research just started with this study.
- In the future it would be interesting to use JavaScript, to obtain additional information about the target system (data such as: computer name, user name, etc.) Another possible line would be the investigation of IP address detection methods, when users use a proxy.

Bibliographic References.

Arndt, M. R., & Actis, F. J. (1996). Method of configuring a valid IP address and detecting duplicate IP addresses in a local area network. https://patents.google.com/patent/US5724510A/en

Arroyo J. Richard. (2016). Análisis de los delitos informáticos por ataque y acceso no autorizado a sistemas electrónicos, tipificados en los artículos 232 y 234 del Código Orgánico Integral Penal en el Ecuador. http://www.dspace.uce.edu.ec/bitstream/25000/5953/1/T-UCE-0013-Ab-121.pdf

Bracho, C., Fabián, C., Pupiales, C., & Suarez, L. (2017). Auditoría de seguridad informática siguiendo la metodología OSSTMMv3: caso de estudio | Maskana. Maskana, 8. https://publicaciones.ucuenca.edu.ec/ojs/index.php/maskana/article/view/1471

De Juventud, E., & De, R. (2017). Jóvenes: bullying y ciberbullying. http://www.publicacionesoficiales.boe.es

García-Maldonado, G., Joffre-Velázquez, V. M., Jesús Martínez-Salazar, G., & Llanes-Castillo, A. (2011). Ciberbullying: forma virtual de intimidación escolar. In Rev. Colomb. Psiquiat (Vol. 40, Issue 1). http://www.scielo.org.co/pdf/rcp/v40n1/v40n1a10.pdf

ISSN: 2600-5859
Vol. 3, N°2.2, p. 80-96, junio, 2020

González García, A. (2015). El ciberbullying o acoso juvenil a través de Internet: un análisis empírico a través del modelo del Triple Riesgo Delictivo (TRD). https://www.tdx.cat/bitstream/handle/10803/384709/AGG_TESIS.pdf?sequence=1

Herrera-López, M., Romera, E. M., Ortega-Ruiz, R., & Herrera, M. (2018). Bullying y Cyberbullying en Latinoamérica. In Revista Mexicana de Investigación Educativa RMIE (Vol. 23). http://www.comie.org.mx/documentos/rmie/v23/n076/pdf/76005.pdf

Ibarra, J. D., & Electrónico, I. (2004). Auditoría tecnológica con fines de seguridad Informática.

Johanna Martínez Molina, K., Pacheco Meneses, J., & Zúñiga Silgado, I. (2009). FirEwall-linux: una solución dE sEguridad inFormática para pymEs (pEquEñas y mEdianas EmprEsas). Revista UIS Ingenierías, 8(2). http://www.

Martinez, F., Caicedo, J., Hernandez, R.,Caicedo, O., & Hurtado, J. (2007). Seguridad basada en parámetros SIM para entornos de comercio electrónico móvil SIM parameter-based security for mobile e-commerce settings. Amicus Curiae, 27(2), 56–64.

Arndt, M. R., & Actis, F. J. (1996). Method of configuring a valid IP address and detecting duplicate IP addresses in a local area network. https://patents.google.com/patent/US5724510A/en

Arroyo J. Richard. (2016). Análisis de los delitos informáticos por ataque y acceso no autorizado a sistemas electrónicos, tipificados en los artículos 232 y 234 del Código Orgánico Integral Penal en el Ecuador. http://www.dspace.uce.edu.ec/bitstream/25000/5953/1/T-UCE-0013-Ab-121.pdf

Bracho, C., Fabián, C., Pupiales, C., & Suarez, L. (2017). Auditoría de seguridad informática siguiendo la metodología OSSTMMv3: caso de estudio | Maskana. Maskana, 8. https://publicaciones.ucuenca.edu.ec/ojs/index.php/maskana/article/view/1471

De Juventud, E., & De, R. (2017). Jóvenes: bullying y ciberbullying. http://www.publicacionesoficiales.boe.es

García-Maldonado, G., Joffre-Velázquez, V. M., Jesús Martínez-Salazar, G., & Llanes-Castillo, A. (2011). Ciberbullying: forma virtual de intimidación escolar. In Rev. Colomb. Psiquiat (Vol. 40, Issue 1). http://www.scielo.org.co/pdf/rcp/v40n1/v40n1a10.pdf

González García, A. (2015). El ciberbullying o acoso juvenil a través de Internet: un análisis empírico a través del modelo del Triple Riesgo Delictivo (TRD). https://www.tdx.cat/bitstream/handle/10803/384709/AGG_TESIS.pdf?sequence=1

ISSN: 2600-5859
Vol. 3, N°2.2, p. 80-96, junio, 2020

Herrera-López, M., Romera, E. M., Ortega-Ruiz, R., & Herrera, M. (2018). Bullying y Cyberbullying en Latinoamérica. In Revista Mexicana de Investigación Educativa RMIE (Vol. 23). http://www.comie.org.mx/documentos/rmie/v23/n076/pdf/76005.pdf

Ibarra, J. D., & Electrónico, I. (2004). Auditoría tecnológica con fines de seguridad Informática.

Johanna Martínez Molina, K., Pacheco Meneses, J., & Zúñiga Silgado, I. (2009). FirEwall-linux: una solución dE sEguridad inFormática para pymEs (pEquEñas y mEdianas EmprEsas). Revista UIS Ingenierías, 8(2). http://www.

Martinez, F., Caicedo, J., Hernandez, R., Caicedo, O., & Hurtado, J. (2007). Seguridad basada en parámetros SIM para entornos de comercio electrónico móvil SIM parameter-based security for mobile e-commerce settings. Amicus Curiae, 27(2), 56–64.

Óscar Fernando Castellanos, Montañez, A. M. F., & Fonseca, S. L. (2007). Bases de la implementación de un modelo de inteligencia para fortalecer el desarrollotecnológico de la industria del software y servicios asociados en Colombia. Ingeniería e Investigación, 27(3), 182–192. https://revistas.unal.edu.co/index.php/ingeinv/article/view/14859

Robert T. Baum. (2003). Methods and apparatus for protecting against IP address assignments based on a false MAC address. https://patents.google.com/patent/US7320070B2/en

Romera, E. M., Ortega-Ruiz, R., Herrera-López, M., Romera, E. M., & Ortega-Ruiz, R. (1996). Revista mexicana de investigación educativa. In Revista mexicana de investigación educativa (Vol. 23, Issue 76). Consejo Mexicano de Investigación Educativa. http://www.scielo.org.mx/scielo.php?pid=S1405-66662018000100125&script=sci_arttext

Sarmiento, O. P., Guerrero, F. G., & Argote, D. R. (2016). Basic security measures for IEEE 802.11 wireless networks. Ingeniería E Investigación, 28(2), 160–167. https://doi.org/10.1109/ITHERM.2016.7517544

Ximhai, R. (2014). Manifestaciones del Ciberbullying por Género Entre los Estudiantes de Bachillerato. Ra Ximhai, 10(2), 235–261. http://www.redalyc.org/articulo.oa?id=46132726010

Zapata, L. (2012). Evaluación y mitigación de ataques reales a redes ip utilizando tecnologías de virtualización de libre distribución. Ingenius.Ups.Edu.Ec, 11–19. http://ingenius.ups.edu.ec/documents/2497096/3033837/Articulo+2.pdf

ISSN: 2600-5859
Vol. 3, N°2.2, p. 80-96, junio, 2020

PARA CITAR EL ARTÍCULO INDEXADO.

Moreano Sánchez, G. V., Ávalos Yuque , E. V., Benitez Bravo, V. H., & Benitez Bravo, A. G. (2020). Métodos electrónicos para obtención de direcciones IP a través de webmail y redes sociales. *ConcienciaDigital*, *3*(2.2), 80-96. https://doi.org/10.33262/concienciadigital.v3i2.2.1247