

Crímenes del Nuevo Siglo: Crímenes Cibernéticos, Abuso Cibernético, Acecho Cibernético, Pornografía Infantil y otros

Carlos R. Ortiz López

Maestría en Ciencias de Computadoras

Dr. Alfredo Cruz

Departamento de Ingeniería Eléctrica y Computadoras y Ciencias de Computadoras

Universidad Politécnica de Puerto Rico

Abstracto — *La tecnología ha acaparado la vida del ser humano a pasos agigantados. Es un hecho que la informática, como parte de dicho surgimiento, también se ha vuelto parte de nosotros. Pero con tal crecimiento, también han surgido nuevas formas de cometer crímenes. Son varios los delitos que pueden hacerse utilizando una computadora, Internet y hasta un teléfono celular. Es un postulado de la Investigación el hecho de que no existe el crimen perfecto, por eso, decidimos realizar nuestro proyecto. En él vemos las clasificaciones de delitos cibernéticos que se han formado en nuestra sociedad. Por medio de entrevistas en distintas entidades, encontramos cómo se está manejando esto en Puerto Rico. Logramos establecer algunas estadísticas que nos muestran tanto el margen de incidentes, como el conocimiento actualizado de esto. También vemos qué medios se utilizan para resolver. Por último, se presentan algunas recomendaciones útiles para protegernos de dicha problemática.*

Palabras Claves — *Abuso Cibernético, Crímenes Cibernéticos, Fraude, Pornografía Infantil.*

INTRODUCCIÓN

Hace 50 años, la tecnología de punta era un televisor de transistores y adquirirlo era muy costoso. Con el pasar de los años, todo evolucionó y hoy día, lo que se veía en aquella cajita maravillosa, y que asombraba a los espectadores, para nosotros es cosa de todos los días. De igual forma ha crecido el mundo de la informática y las computadoras, exorbitantemente. Tanto adelanto le ha hecho la vida más fácil al ser humano pero también abrió nuevos métodos de cometer crímenes y/o facilitarlos. Desde que se inicia la investigación de un delito, se presume que no existe uno perfecto y que el criminal

deja huellas que llevan a su captura. De igual forma, aquel que se comete utilizando medios tecnológicos tiene su marca. Existen herramientas que descubren ese detalle que, quizás por falta de conocimiento o preparación suficiente, no se puede obviar.

Hay personas que utilizando Internet, contactan menores de edad y los manipulan para hacer cosas indebidas. Otros, que tienen posiciones privilegiadas en la sociedad, o empresas que manejan mucho dinero, utilizan información importante para generar altas sumas de dinero. Otros simplemente cometen delitos a diario, pero por cosas o transacciones que se hacen por medio de computadoras, se puede rastrear día a día lo que hicieron o planearon. Todo eso es posible gracias a herramientas o softwares diseñados para descubrir lo que de forma simple no se puede. Una foto borrada, un correo electrónico eliminado o un documento que se ha codificado, puede recuperarse utilizando dichos medios. Investigamos en nuestro proyecto nuevas tendencias criminales y como pueden encontrarse.

Nuestro proyecto fue dirigido a investigar cuantas clasificaciones de delitos cibernéticos existen. Descubrimos por medio de entrevistas en entidades gubernamentales que no sólo existen, sino que el desconocimiento de nuestra sociedad es mayor al que se pudiera pensar. Después de todo, estamos en el siglo XXI, ¿hay pocas cosas que pudiéramos desconocer?, si las hay, y entre ellas están las modalidades de crímenes cibernéticos. ¿Hay formas de descubrir las personas que delinquen por medio de la tecnología?, sí las hay, y hasta algunas de esas formas están al alcance de nuestras manos. Vimos que con el conocimiento adecuado, podemos obtenerlas.

INVESTIGACIÓN

Crímenes Cibernéticos — No hay duda que la tecnología ha crecido, y continúa a pasos agigantados. Aunque muchos consideren que en los últimos años se ha estancado, no se puede acertar con gran seguridad que sea así. Con el crecimiento de beneficios también llegan las vicisitudes. El surgimiento del mal uso de los adelantos es inevitable, especialmente en el área de la informática. La tendencia a cometer crímenes a través de estos medios cada vez es mayor. Por tal motivo, la actualización y mejoramiento de las herramientas forensicas son muy importantes. El lograr con su uso encontrar, detener y sentenciar a aquellos que hacen mal a otros con la tecnología, es sumamente importante.

La creación de Internet aparenta ser una de las más grandes en la historia de la humanidad. Ha logrado que el mundo, que antes parecía enorme, se vuelva pequeño y hasta se podría decir insuficiente para las personas de hoy. Internet nos brinda una gama de oportunidades, facilidades y conexiones que nuestros abuelos jamás hubieran imaginado. Podemos utilizarla para buscar trabajo, comprar, estudiar y para comunicarnos con otras personas. Esto último usando las llamadas redes sociales, que hacen que decenas, centenas y miles de personas de diferentes partes del planeta, se conozcan, interactúen y hasta se enamoren y unan sus vidas. Son enormes los usos que le han dado a dichas redes, pero, también de mal uso han sido objeto. Entre las más famosas podemos mencionar: Facebook, Twitter, Skype y otras. Todas funcionan con métodos parecidos y todas en algún momento han sido medios para delinquir.

Cuando una persona utiliza una red social para proferir palabras soeces, insultos, amenazar, humillar, grabar sin autorización o algo parecido a cualquiera de las mencionadas, está cometiendo un delito [1]. Muchos pudieran pensar que tal práctica se daría mayormente en jóvenes inmaduros pero, alarmantemente se da a cualquier edad. Hay diversas razones para llevar a cometer estos actos, pero las principales traídas en escala son: 1) relaciones

amorosas; 2) informaciones personales que se divulgan a propósito; 3) amistades que se rompen; entre otras. El mayor problema que se obtiene es el hecho que las redes sociales están tan proliferadas, que casi el 80% de las personas en Puerto Rico son parte de ellas. Por tal motivo se hace casi imposible controlar dicha práctica. En la Figura 1 podemos observar una publicación que aparece en Facebook en la cual, escriben múltiples improperios acerca de la dama que aparece en la foto.



Figura 1

Publicación Sacada de Facebook

Podemos pensar que todos los que se hacen parte de una red social, saben a lo que se exponen por medio de ellas, pero nada más lejos de la verdad. Todo lo mencionado está catalogado como crimen cibernético, pero en la mayoría de los casos en nuestra isla lo canalizan como otros. Por ejemplo, un caso en el que una persona insulta a su pareja por Internet, lo llevan al Tribunal como Violencia Domestica, y así se pierde el hecho de su naturaleza. Esto debido a que en vez de sólo un cargo, puede aplicarse dos, pero basado en el hecho de que la Ley Orgánica, o Ley Especial, está dirigida a una

conducta en específico, la misma absorbe como parte de sí cualquier hecho que se tipifique en el Código Penal.

Hay personas que se valen de la información que se brinda en las redes sociales, o que logran adquirir información personal de otras y luego, con dichos datos las extorsionan para adquirir algún beneficio, ya sea económico, sexual o de otra índole. Estas mencionadas extorsiones [2] pueden lograrse al obtener fotos, documentos o grabaciones importantes, y que quizás esas personas no deseen que salgan a la luz. En Puerto Rico, ésta práctica se ha vuelto muy común, especialmente entre la comunidad de confinados. Estos adquieren teléfonos celulares clandestinos, los cuales les dan acceso al uso de Internet y con ello, pueden cometer dichos delitos. Estos teléfonos que logran entrar a las Instituciones Penales siempre son los llamados servicios pre-pagados, las compañías celulares no llevan una documentación de su uso, por lo que, nunca es posible acceder a tales delincuentes. Lamentablemente lo más que se logra en nuestra isla es procesar por el Artículo 2 de la Ley 15 del 18 de febrero de 2011, el cual tipifica como delito el poseer el artefacto en dicho lugar, y el otro crimen queda impune.

Recientemente en Puerto Rico hubo un caso muy mencionado de extorsión, el cual agradadamente se pudo dar con los responsables. El mismo fue de una banda, entre confinados y civiles que por medio de Internet, lograron acceder a información que los llevó a extorsionar a varias agencias del Gobierno. Entre dichas agencias se encontraba la Universidad de Puerto Rico y algunos Municipios [3]. La información adquirida por medio de Internet, los llevó a hacerse pasar por el Sr. Jorge Colberg, Secretario de Asuntos Públicos del Gobierno, y mediante llamada telefónica, lograron que les emitieran cheques que luego trataron de cambiar.

Continuando con lo expuesto, en estos días se ha desatado una tendencia en las redes sociales que no se había visto nunca. Personas que han obtenido fotos o videos comprometedores, han expuesto los mismos difundiéndolos en Internet. Puerto Rico aún

no cuenta con una Ley que haga de dicha práctica un delito, pero ya hay un movimiento para lograrlo. Las razones que llevan a dicho comportamiento pueden variar, desde despechos amorosos, hasta meramente realizar una broma de mal gusto. El problema puede agravarse si a raíz de tal suceso, los perjudicados reaccionan de forma incorrecta. Muchos esperan lograr que se apruebe dicha Legislación y convertirlo en otra modalidad de crimen cibernético, solo el tiempo dirá. Un caso muy sonado de esto es el de un video en el cual aparecen dos Agentes de la Policía de Puerto Rico sosteniendo relaciones sexuales [4]. Hay quienes aseguran que el mismo llegó a las redes por medio de la esposa del hombre, quien lo encontró y por venganza a ella, difundió su contenido. Esto último no fue confirmado.

Uno de los más aterradores crímenes o quizás el peor es la práctica de Pornografía Infantil [5]. Esta modalidad lleva a personas a adquirir material de contenido sexual en el cual está envuelto un menor de edad, y difundirlo por las redes sociales o Internet. Propósitos para esto hay muchos: trata de niños con fines de prostitución, ganar dinero con dicho material, venganza, desviaciones mentales, entre otros. Estos casos no tienen una esfera social específica, ya que se puede dar entre personas de cualquier nivel. En ocasiones, aun conociendo lo que pasa, hay personas que callan por miedo o indiferencia, y tales actos los convierten en cómplices.

En relación a tales sucesos, la Policía de Puerto Rico no tiene una estadística precisa ya que cuando se obtiene conocimiento del mismo, el 90% de ellos son adjudicados a foros federales, quienes se encargan de procesarlos. Una de las variantes de esto es el utilizar las redes sociales para manipular y convencer a niños a hacer cosas que no son permitidas. Les piden fotos a cambio de dinero, videos y hasta les hacen creer que hay amor entre las partes y así logran obtener sexo. José R. Arriaga fue un locutor radial y periodista, quien fue acusado por agresión sexual contra un menor [6]. Alegadamente éste conoció al joven a través de una red social, le pedía fotos y lo convenció de regalarle una cámara para poder obtener videos del mismo. Indicó el

joven, que en una ocasión tuvo la intención de cometer suicidio debido a todo lo ocurrido. En el Tribunal, el caso no prosperó debido a tecnicismos legales.

ENTREVISTAS Y RESULTADOS

A modo de profundizar la investigación, surgió la oportunidad de realizar varias entrevistas interesantes, las cuales arrojaron un grado mayor de conocimiento acerca de todo lo aquí expuesto. En una conversación con el Sargento Luis Maldonado, de la División de Crímenes Cibernéticos de la Policía de Puerto Rico, pude encontrar que dicha división sólo se ocupa de brindar apoyo a los Precintos en sus casos. De surgir un delito cometido mediante redes o medios cibernéticos, el Agente solicita una supina, entiéndase orden del Fiscal, para que la persona sospechosa brinde claves, números secretos y accesos en sus dispositivos. Tal protocolo es a tenor con la Sección 10 del Artículo 2 de nuestra Constitución, el cual otorga una expectativa de privacidad al ciudadano. Con la mencionada orden se llega a la información sin violar derechos adquiridos, misma que utilizan para elaborar y llevar el caso a los Tribunales.

Muy amablemente, el Supervisor de tal División nos facilitó unos datos estadísticos, los cuales nos indican que en el 2013, le fueron solicitados servicios para aproximadamente 909 casos. Los datos arrojados de servicios solicitados hasta mayo de 2014 indican un número aproximado de 750, lo que claramente refleja un aumento considerable. Se entiende que tal cifra sólo corresponde a los servicios prestados a Agentes de Precintos ya que, como pudimos ver antes, hay muchos casos que se resuelven por otros canales. En la Figura 2 podemos apreciar dichos datos obtenidos. El Sargento, en adición, nos mencionó que a raíz de su investigación en el 2010, se pudo resolver un caso de amenazas al Secretario de Estado en aquel entonces, Sr. Kenneth McClintock, logrando llevar el mismo a Tribunales con resultados positivos.



Figura 2

Datos ofrecidos por la División de Crímenes Cibernéticos de la Policía de P.R. sobre los Servicios Ofrecidos

Luego de entrevistar a 10 Agentes de la Policía de Puerto Rico, obtuvimos los siguientes datos: todos en algún momento escucharon el término, de ellos 7 conocen que existe la División de Crímenes Cibernéticos y 6 pensaban que esto sólo se refería a Pornografía Infantil. En la gráfica que se muestra en la Figura 3 podemos observar dichos datos. Luego de la encuesta, se interesaron en obtener más información sobre el tema y saber cómo funciona la División. Algunos hasta asociaron uno que otro caso investigado y entendieron que aplicaba dicha clasificación. Todos llegaron a la conclusión que al igual que la sociedad, había que evolucionar y adaptarse en relación a la tecnología. En ocasiones el problema radica en que aún hay personas que no se interesan en educarse sobre la informática y en su crecimiento.

Se logró entrevistar al Fiscal Gabriel Reyes Vázquez, asignado a la Región de Bayamón, quien muy cordialmente nos indicó que en cada región en Puerto Rico, se estaba asignando un Fiscal que trabaje exclusivamente con estos crímenes. La razón para ello ha sido la proliferación de los mismos en nuestra isla. También están gestionando asignar un agente de apoyo para las investigaciones. Nos comentó que de los delitos mencionados, el acoso y maltrato son los más comunes. También nos confirmó que la Pornografía Infantil se trabaja a nivel Federal y que aún el día de hoy hay personas que desconocen que estos delitos se tipifican como tal.

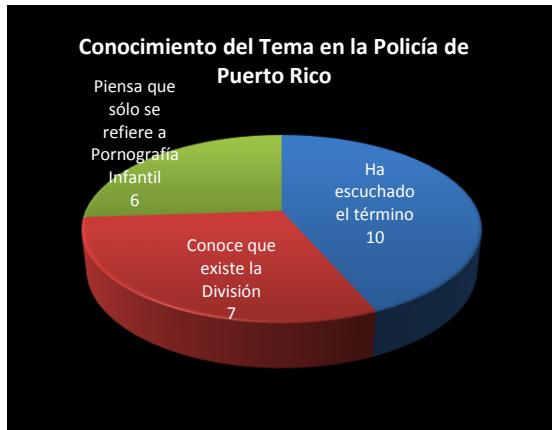


Figura 3

Datos Reflejados por la Encuesta Realizada a Agentes de la Policía de P.R. sobre su Grado de Conocimiento Acerca de los Crímenes Cibernéticos

Para seguir profundizando, entrevistamos al Juez Municipal y Coordinador de Sala de Investigaciones del Tribunal de Bayamón. Este nos confirmó que al menos ante su consideración, no se ha llevado caso alguno tipificado como crimen cibernético. Que sí ha visto casos de Violencia Doméstica, acecho y/o maltrato bajo otras leyes, y que el hecho de utilizar medios informáticos para esto, solo se ha presentado como parte de una prueba sobre lo otro. Le pregunté a 5 Jueces acerca del tema, obteniendo los siguientes datos: 4 sabían a qué me refería al mencionar “crímenes cibernéticos”, ninguno ha visto un caso que haya sido específicamente del tema y en nuestra judicatura aún no se ha dado ningún taller acerca de esto.

Todo lo antes expuesto nos lleva a buscar razones para el fenómeno que se da en nuestra isla. Entrevistamos al Maestro Javier Torres, educador de escuela elemental a superior, quien lleva 6 años en el Departamento de Educación fungiendo como Maestro de Educación Física. El señor Torres nos relató un caso en particular en el cual dos bandas de féminas en la escuela en la que trabajaba, llevaban tiempo presentando problemas. Uno de los bandas utilizó el Facebook para difundir unas fotos en las que aparecían muñecas, parecidas a las niñas del otro, y las mismas estaban amarradas por el cuello y con una tinta que emulaba sangre. Tal suceso llevó a citar a los padres y llegar a unos acuerdos. Al preguntar por qué no fue llevado al Tribunal, nos

confirma que a tenor con las enmiendas de la Ley Orgánica, los asuntos escolares deben primariamente tratar de resolverse a nivel administrativo.

Para lograr entender que posición ocupan los Maestros Escolares que cuidan de nuestros niños, en medio de todo lo expuesto, me di a la tarea de entrevistar a 5 Maestros de diferentes niveles. Cada uno me contestó unas preguntas que me revelaron los siguientes datos: 1) los 5 en algún momento escucharon acerca de los crímenes cibernéticos, 2) dos de ellos se dieron con alguna situación catalogada como crimen cibernético; 3) dos de ellos pensaban que el término sólo se refería a la Pornografía Infantil; 4) cuatro de ellos entendieron que hace falta talleres informativos; 5) tres de ellos coincidieron en que no se debería mantener como asunto administrativo el hecho de lidiar con dichos casos.

Para tratar de adquirir una estadística un poco más precisa, y tomando en cuenta que el mayor uso de Internet hoy día es por medio de teléfonos celulares, entrevistamos a empleados de las diferentes compañías de la isla. Encontramos que mensualmente se solicitan en dichas empresas aproximadamente sólo de 45 a 60 supinas para investigaciones. Solo T-Mobile tiene en sus servidores, la forma de almacenar los mensajes de texto de sus clientes, pero por un tiempo limitado. Para ellos es posible, ya que su cartera de clientes no es tan grande como la de las otras empresas. Tanto Sprint como AT&T, tienen su departamento de seguridad corporativa fuera de la isla, lo que nos lleva a que en caso de una investigación, el oficial a cargo de representarlas en el Tribunal, solo posee información superficial, que poco ayudaría a resolver un caso. Y Claro sólo puede ofrecer datos de llamadas entrantes y salientes, pero no del uso detallado del servicio de Internet.

Entendiendo que hace falta tener datos más reales acerca del tema, hice una encuesta con jóvenes entre las edades de 12 a 28 años, la cual arrojó los siguientes datos: 7 de cada 10 han sido víctimas de algún incidente en su Facebook. Sólo 1 prefiere no tener cuenta en redes sociales y los mencionados

como agredidos, resolvieron simplemente eliminando de su conexión a la persona con la cual tuvo el altercado. Dividiendo los datos por generaciones, entre las edades de 12 a 18 años, 8 de 10 víctimas han sido féminas mientras que 2 han sido varones y entre las edades de 19 a 28 años, 7 de 10 han sido féminas mientras que los restantes han sido varones. Dichos altercados han sido sólo de palabras por lo que nos deja con un número bajo de personas las cuales sienten un verdadero temor debido a problemas o amenazas. La Figura 4 nos muestra más a fondo la estadística mencionada.

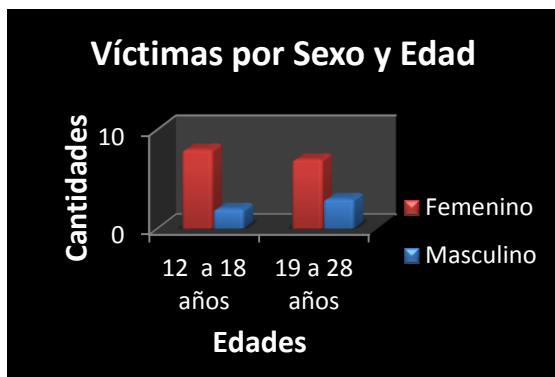


Figura 4

Datos que Reflejan la Estadística de Incidentes entre Jóvenes

Continuando con la Investigación, me di a la tarea de llegar hasta el Edificio Federal en Puerto Rico. Allí tuve la oportunidad de conversar con el Sr. Edgar Lorenzo, quien labora como Científico en Informática por espacio de dos años. El Sr. Lorenzo me comentó que estudió en la Universidad Politécnica de Puerto Rico, específicamente en la concentración de Seguridad. Bajo la información que me brindó, me indicó que a diario son consultados por las autoridades locales referente al área de los crímenes cibernéticos. También brindan apoyo técnico y cuando toca el momento, asumen jurisdicción según amerite el caso. Al tocarle el tema de la Pornografía Infantil, me indicó que por motivos de confidencialidad por sus métodos de investigación, no podía abundar mucho, pero que una de las cosas que sí hacen en el F.B.I es que a menudo, navegan en conocidos lugares haciéndose pasar por menores para interceptar Depredadores Sexuales. También me comentó que entre las herramientas de Forénsica que utiliza en su trabajo,

la más frecuente es FTK y otras que ellos mismos elaboran a su conveniencia. Por ultimo me refirió a una página de Internet que pertenece a la Agencia para datos estadísticos.

Ya que en la Oficina del F.B.I me indicaron que no hay un tipo de crimen más común que otro, entré a la página referida para obtener más datos [7]. En dicha Agencia, tienen tipificados 20 tipos de delitos cibernéticos, entre los que figura el robo de identidad, fraudes con tarjetas de crédito, extorsión, inversiones, y otros. Según sus datos, en el 2013 recibieron 262, 813 quejas, de estas, el 52% fue de varones y el 47% de féminas. De los delitos en los que hubo dinero envuelto, las pérdidas ascendieron a \$781, 841,611. De todo esto, Puerto Rico reportó un 0.04% con 101 casos investigados, ocupando la posición #41 de 50. En aquellos casos en que no hubo dinero envuelto, sino víctimas de delitos, Puerto Rico reportó un 0.21% con 550, ocupando la posición #8 de 50 y en casos en que se perdieron las víctimas, Puerto Rico reportó un 0.23% con 271 ocupando la posición #9 de 50. Luego de todo esto, puedo deducir que en la Agencia Federal no están brindando detalles sobre algunos de los temas debido a la delicadeza del mismo, pero, al menos obtuve información sobre otras áreas de interés.

USO DE HERRAMIENTAS DE FORÉNSICA

Buscando información sobre los métodos investigativos, llegué al Instituto de Ciencias Forenses, organismo local que se encarga de las Investigaciones Criminales. Allí pude hablar con la Sra. Julia Hernández, quien lleva laborando en dicha entidad alrededor de 13 años. Ella me comentó que cuentan en su área de trabajo, con varias herramientas de Forénsica de las más conocidas. Estas se utilizan para investigar casos que surgen, pero que dicha área en nada se parece a lo que puede verse en series de TV, por el contrario, son más limitadas en cuanto a máquinas para trabajar. El uso de cada herramienta es de acuerdo al caso en específico pero que la más utilizada es EnCase. Luego de abundarle sobre la posibilidad de ProDiscover para encontrar información, me indicó que adquirieron la misma gratuitamente a través de

Internet pero que no la utilizan. Por último, me comentó que no cuentan con datos estadísticos. Esto me llevó a buscar otras alternativas de búsqueda de información.

Tuve la oportunidad de comunicarme vía email con el Dr. Jeffrey Duffany, profesor de la Universidad Politécnica de Puerto Rico. Lleva alrededor de 3 años ofreciendo el curso de Computer Forensics, dirigido al aprendizaje de métodos de investigación forense en informática. El mismo me indicó que de recomendar alguna herramienta, la misma sería Sleuth Kit ya que puede adquirirse gratuitamente. Entendemos que dicha recomendación sería para un estudiante en desarrollo pero al abundarle sobre un investigador profesional su opinión cambió. El Dr. Duffany entiende que las tres mejores herramientas que tiene el mercado para dicha área lo son ProDiscover, EnCase y FTK, lo que nos lleva a tener ya una idea muy clara de las herramientas de Forénsica y las tendencias en relación a ellas.

No tuvimos la oportunidad de encontrar un Investigador Forense privado pero sí encaminarnos en otras vías. Hace varios años, el ex Capitán de la Policía de Puerto Rico, y ex Comisionado de la Policía Municipal de San Juan, Sr. Hilton Cordero, fue acusado de pornografía infantil [8]. Su caso fue llevado tanto en el foro estatal como en el foro federal. Su defensa, muy amablemente nos contestó algunas preguntas de las cuales obtuvimos datos importantes. Dichos datos nos confirmaron que la evidencia fue adquirida por técnicos federales pero jamás le indicaron qué herramientas utilizaron, ni pudo ser debatida la metodología.

Toda esta información nos lleva a entender que: 1) en Puerto Rico, las entidades estatales todavía están distantes en el área de investigaciones forenses en informática; 2) los laboratorios disponibles no cuentan con tecnología de punta para realizar las investigaciones necesarias; 3) la alternativa idónea para quien desee una investigación de altura es un técnico privado; 4) que quizás debido a esto, como ocurrió en el caso presentado del locutor radial [6], muchos otros no serán sentenciados ya que la falta de una preparación adecuada continuará

produciendo errores; 5) todos los caminos nos llevan a ver que entre las alternativas presentes a la hora de escoger una herramienta, sólo tenemos EnCase o FTK como marcas principales.

VISTA BREVE DE UNA HERRAMIENTA DE FORÉNSICA

El manejo de una herramienta de Forénsica requiere estudio y aprendizaje. Veamos por ejemplo ProDiscover, una vez obtenido e instalado en la computadora, para recuperar cierta información con él, debemos primeramente tener los archivos en una memoria USB o conectar la unidad a trabajarse por medio de un puerto. Para guardar los datos obtenidos, debemos tener una carpeta dirigida a dicho fin y debidamente identificada, a modo que no surja confusión con otras. La Figura 5 muestra un ejemplo del archivo llamado ProDisc, utilizado para este trabajo.

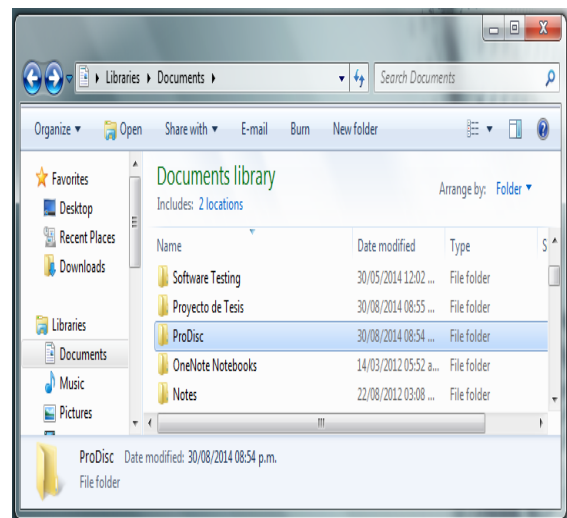


Figura 5
Archivo ProDisc Utilizado para Guardar Datos Recuperados de ProDiscover

Luego vamos al menú de trabajo de ProDiscover y en Archivos, escogemos crear uno nuevo, como se puede apreciar en la Figura 6. Aparecerá una pantalla que nos pide unos datos básicos, como número del Proyecto, archivo a guardarse y descripción del mismo, los cuales deben ser completados. Podemos verla en la Figura 7.

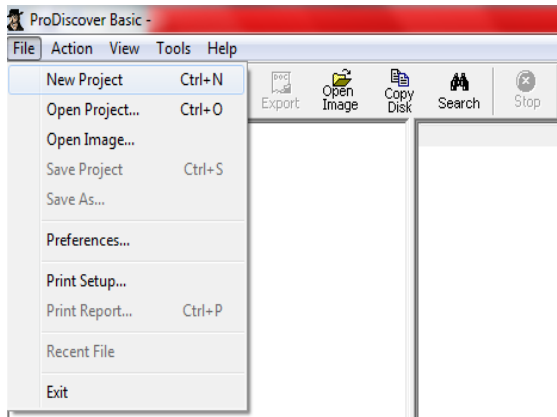


Figura 6

Alternativa Archivo con la Selección de Nuevo Proyecto

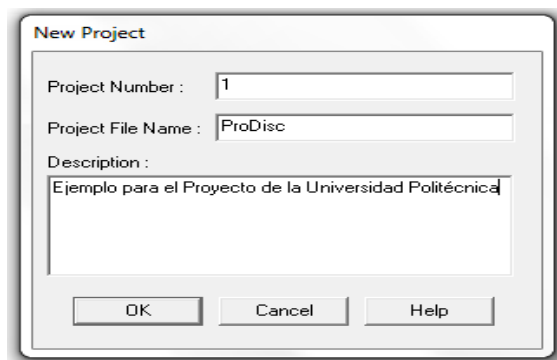


Figura 7

Datos Necesarios para Nombrar un Trabajo de Investigación en ProDiscover

Una vez hecho esto, se presentará una lista de trabajo, de la cual se escogerá la alternativa Capturar Imagen. Aparecerá otra pantalla que pide unos datos, como escoger el dispositivo que se trabajará, el destino a guardarse, el nombre del técnico realizando la tarea y otros, los cuales deben ser completados. Las Figuras 8 y 9 nos muestran todo esto en detalle. Una vez culmina éste proceso, la herramienta comenzará a hacer una copia de los datos guardados de una memoria USB, que utilizamos para realizar el trabajo aquí descrito. La misma almacenará en el archivo destinado para ello los hallazgos. Dependiendo del peso que tenga el archivo a trabajar, la herramienta trabajará más rápido o lento.

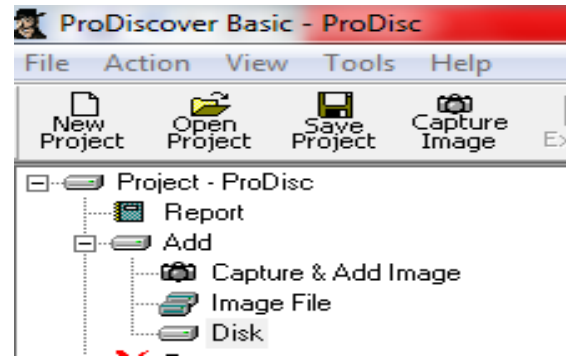


Figura 8

Alternativa Capturar Imagen la cual nos Ayuda a Realizar Trabajos en ProDiscover

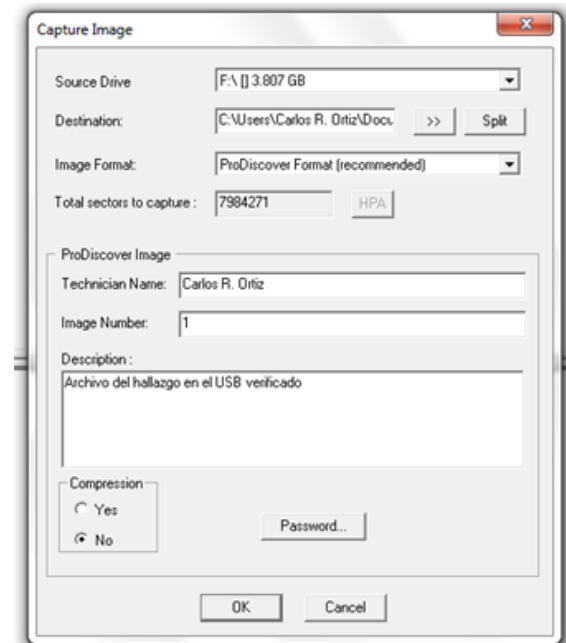


Figura 9

Pantalla de Datos para Capturar la Imagen Necesaria

La Figura 10 nos muestra la pantalla que indica el tiempo restante para culminar la labor. Al terminar el análisis, accediendo a través de las alternativas correspondientes, se puede hacer el estudio necesario de la imagen capturada de la memoria utilizada. De acuerdo al modo en que aparecen los datos, quizás se requiera otros métodos adicionales para recuperar los datos deseados. Esto debido a que pueden aparecer como archivos puestos sobre otros o imágenes fragmentadas que necesitan unirse nuevamente. De ocurrir esto, el proceso de recuperación se vuelve más elaborado ya que habría que trabajar entonces con ciertos sectores de los

datos. La Figura 11 nos muestra que podemos llegar a los datos recuperados a través de la vista en trozos.



Figura 10

Pantalla que nos Muestra el Tiempo Restante para Culminar el Trabajo

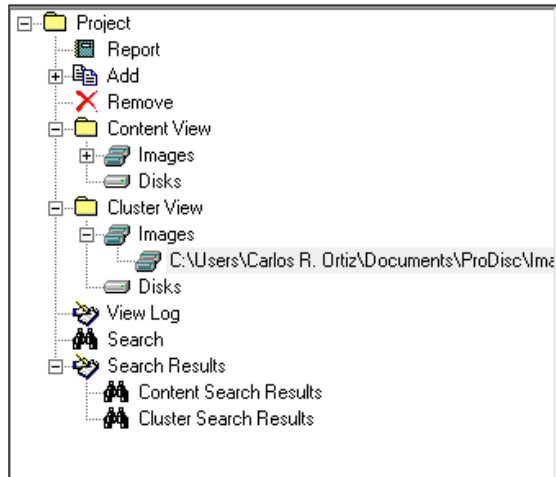


Figura 11

Alternativa de Vista en Trozos, se Utiliza para Llegar a los Datos Recuperados

En las Figuras 12 y 13 vemos que la herramienta nos muestra los sectores de la memoria que están en uso, disponibles o sobre escritos. Podemos distinguirlos utilizando la leyenda.

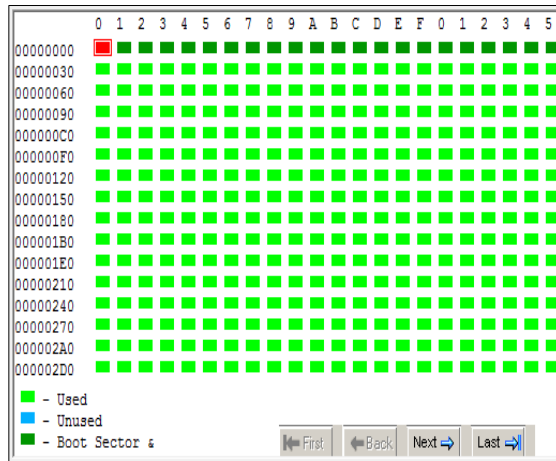


Figura 12

Leyenda de la Herramienta con sus Sectores, Aquí se Apprecia que los Mismos están en Uso, los de la Primera Fila están sobre Escritos

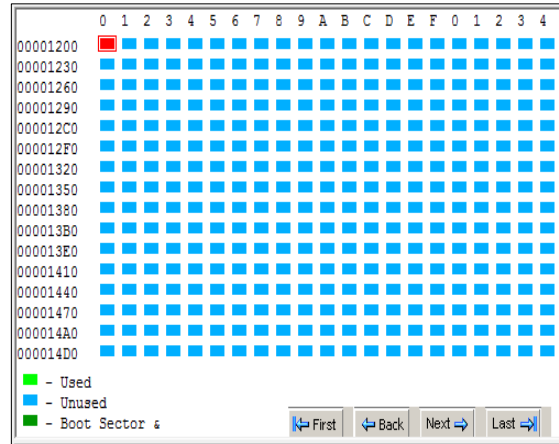


Figura 13

Sectores de la Memoria con Espacio Disponible, Cambiamos de Sectores Utilizando las Flechas Azules

Para trabajar los datos se necesita tanto la vista de sectores segmentados, como el número hexadecimal y/o su equivalente ASCII. La Figura 14 nos muestra dicha información recuperada del trabajo realizado.

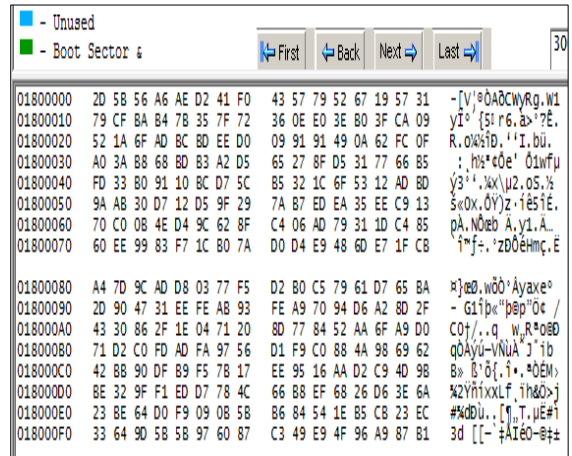


Figura 14

Datos Presentados en su Forma Hexadecimal, a la Derecha de la Pantalla Aparece su Equivalente ASCII

RECOMENDACIONES

Entre las mejores recomendaciones a las personas y en especial padres de niños para evitar todo esto: 1) debemos analizar cuidadosamente nuestros actos, ya que nos pueden traer consecuencias; 2) no se puede ofrecer muchos detalles privados en las redes sociales; 3) debemos supervisar el uso de Internet por parte de los niños, para que personas inescrupulosas no puedan atentar

contra su integridad; 4) a la hora de hacer compras en línea, debemos informarnos sobre los ofrecimientos de seguridad para así proteger nuestras finanzas y cuentas; 5) se debe promocionar mediante campaña en todos los medios, la prevención de éste tipo de comportamiento. La Figura 15 nos da un ejemplo de un buen Logo de campaña, el cual se podría utilizar para crear conciencia en nuestros ciudadanos.



Figura 15
Logo de Campaña contra la Pornografía Infantil

CONCLUSIÓN

Hemos podido observar que Puerto Rico aún no está al tanto de los alcances reales que puede tener la tecnología en nuestra sociedad de forma negativa. Vemos que aun siendo víctimas de crímenes cibernéticos, las personas se vuelven indiferentes y sus soluciones a estos, son superficiales. Apenas ahora, las autoridades locales están comenzando a actualizarse para hacer frente a ésta tendencia. Los números, por más disyuntivas existentes, reflejan solo una cosa, aumento de casos exponencialmente. No podemos seguir siendo inocentes porque cada día son más los efectos contundentes.

En relación a los hallazgos acerca de los métodos para realizar investigaciones, definitivamente las escenas que se presentan en T.V. sobre herramientas y laboratorios de Forénsica, sólo es una presentación exagerada de la realidad. Contamos con métodos para investigar crímenes cibernéticos, pero la ficción sólo aumenta lo que en

verdad tenemos. Por último, no debemos obviar las recomendaciones, nos pueden evitar problemas.

REFERENCIAS

- [1] Abuso Cibernético. Recuperado el 25 de mayo de 2014 de <http://en.wikipedia.org/wiki/Cyberbullying>.
- [2] Acecho Cibernético. Recuperado el 25 de mayo de 2014 de <http://en.wikipedia.org/wiki/Cyberstalking>.
- [3] López, K., "Investiga la UPR entrega de cheques por timo", *El Nuevo Día.com*, 26 de marzo de 2013. Recuperado el 28 de mayo de 2014 de <http://www.elnuevodia.com/investigalautregadechequesportimo-1477805.html>.
- [4] Bigio, A., "Mujer policía va a polígrafo si su pareja en video sexual también va", *Noticel.com*, 31 de marzo de 2014. Recuperado el 28 de mayo de 2014 de <http://www.noticel.com/noticia/158161/mujer-policia-va-al-poligrafo-si-su-pareja-en-video-sexual-tambien-va.html>.
- [5] Pornografía Infantil. Recuperado el 25 de mayo de 2014 de <http://en.wikipedia.org/wiki/Childpornography>.
- [6] Vázquez, E., "Testigo narra encuentro con José Raúl Arriaga", *Primera Hora Online*, 19 de enero de 2012. Recuperado el 28 de mayo de 2014 de: <http://www.primerahora.com/noticias/policia-tribunales/nota/testigonarraencuentroconjoseraularriaga-603391/>.
- [7] Datos Estadísticos del F.B.I., 2013. Recuperado el 17 de junio de 2014 de <http://www.ic3.gov/default.aspx>.
- [8] Cobián, M., "Sentencian a Hilton Cordero a 10 años de prisión en caso federal de pornografía infantil", *Primera Hora Online*, 18 de noviembre de 2011. Recuperado el 28 de mayo de 2014 de <http://www.primerahora.com/noticias/policia-tribunales/nota/sentencianahiltoncorderoa10anosdeprisionencasofederaldepornografiainfantil-970953/>.