Virtual Forum Against Cybercrime

Newsletter

February
Issue: 09

Editorial

VFAC

“Although for such a beastly month as February, twenty-eight days as a rule are plenty, One year in every four his days shall be reckoned as nine and twenty.” *W. S. Gilbert - The Slave Of Duty 1879.*

2012 is of course a leap year, providing us with an extra day in which to meet our deadlines.

Through this newsletter we are very much looking to promote a sharing of ideas and a greater understanding of cybercrime issues from the multitude of viewpoints that the globe offers. We would like to wholeheartedly thank the contributors to this issue and we are very proud to feature their fine articles. The esteemed Melia Kelley provides an excellent practical example of scientific process in investigation and the well respected Deberati Halder gives insight into the complex intertwining of legal and moral issues currently arising in India.

We encourage you all to submit any and all ideas and musings that may be of value to this publication and of course urge you to make good use of the VFAC website, as well as connecting with us on facebook and twitter.

Recent Publication

Middle East

Book

Cybercrime Legislation in The Middle East

The Road not Traveled

Mohamed N. El Guindy and Faisal Hegazy

http://netsafe.me/2012/02/28/cybercrime-legislation-in-the-middle-east/

Investments by MENA countries in ICTs is expanding annually and even overtaking the rest of the world. Millions of home users and businesses in the region are joining the global cyberspace. Virtually all modern services depend on ICTs and in a way or another are connected to cyberspace which considered one of today’s battlefields (Air, Land, Sea, Space, and Cyberspace). Failure to understand this situation will leave Middle Eastern countries vulnerable to all types of attacks. Due to lack of technical and legislative capabilities, our region is expected to become the biggest source and target for cybercrime in 21st century. Drafting a cyber law or even dedicated cybercrime legislation is not the solution, but a part of it. An extensive study of cybercrime phenomenon and its consequences on the region should be considered along with cyber security issues. Although most countries in the region don’t have specific legislation for cybercrime or cyberspace, we still can see few countries with little progress in the field. In this research, we will investigate Cybercrime related issue in the region and will study legislation with overview on each country.

Conferences, etc.

Events

Black Hat USA 2012	United States	2012-07-21
British Society of Criminology Conference 2012: Criminology at the Borders	United Kingdom	2012-07-04
24th Annual FIRST Conference on Computer Security Incident Handling	Malta	2012-06-17
IFIP SEC2012 Conference	Greece	2012-06-04
ERA Conference Fighting Cybercrime: Between Legislation and Concrete Action	Italy	2012-05-24
IEEE Symposium on Security & Privacy	Afghanistan	2012-05-20
ASIACCS 2012: 7th ACM Symposium on Information, Computer and Communications Security	South Korea	2012-05-01
3rd Euroforensics Conference	Turkey	2012-03-29
SANS 2012	United States	2012-03-23
The Inaugural Cyber Crime Symposium	Australia	2012-03-01

Virtual Forum Against Cybercrime

Issue: 09
Feb

News & Trends

News

(2012-02-01) Dutch Supreme Court: Forcing teen to drop virtual objects in online game was real-world theft

The Dutch Supreme Court ruled that the those whom physically assaulted and threatened a teen to force him to drop items in a game, so that they retrieve those items committed theft. The court stated that the possession of the virtual items in the virtual world has an intrinsic value because of the time and energy that the gamer had invested in obtaining them. The case illustrates not only how events in a virtual space can transfer to real life crime, but also how events in real life can form part of a crime in cyberspace. Courts internationally have yet to establish a firm understanding of the value of items in virtual worlds.

(2012-02-23) Firm entitled to serve legal documents via Facebook, High Court rules

Mr Justice Teare of the High Court in the United Kingdom ruled that documents could be served via Facebook, in a case where the postal address of the man was uncertain and after hearing evidence that the man was active on the site and that it was an authentic account belonging to him.

(2012-02-29) Security firm targeted by Anonymous gives up the ghost

IT Security Firm HBGary, known as one of the first major casualties of the hackitvist collective Anonymous has been acquired by rival company Man Tech International. HBGary rose to infamy when the then CEO Arron Barr threatened to reveal information about the members of Anonymous, prompting the group to compromise the company's systems an release confidential emails to the public. The reputation of the firm was irreparably damaged, precipitating the failure of the company. This case illustrates the implications of taking the risks that can be posed by online groups too lightly.

(2012-02-09) File Sharing in the Post MegaUpload Era

MegaUpload traffic represented 30-40% of online file sharing, and hours after the website's founder was arrested global internet traffic fell by an amazing 2-3%. Other file sharing sites have also reinforced anti-piracy measures or closed operation in fear of receiving similar treatment as Mega Upload CEO, Kim Dotcom. However, research by Deepfield Networks suggests that in the time since the file sharing community has shifted its traffic to foreign servers, and are potentially creating a greater drain on the more expensive intercontinental links. The initial actions against torrent sites caused a change in sharing systems such as the use of magnet links and even the revival of usenet. Similarly, downloads of software for true peer to peer file sharing on point to point dark networks (such as the open source program retroshare) has recently increased. It could suggest that any 'success' in reducing content crime by the arrest of Kim Dotcom may be short lived and have only caused a shift of means.

Digital Forensics

Article

Foreword

The need for Digital Investigators around the world to communicate is often spoken about in a general sense. The issues surrounding discussing work that is generally sensitive in a way that does not compromise the effectiveness of the work or the ethics or the investigator often stifles the kind of conversations that should be taking place. Well known Digital Forensics Bloggers such as Corey Harrell (journeyintoir.blogspot.com) have been working to change this by sharing their experiences in investigations, just cutting out the aspects of the case that are overly specific.

Melia Kelley, a seasoned investigator in the United States of America has contributed a 'Case Experience' in the inimitable style of her blog; Girl, Unallocated (http://girlunallocated.blogspot.com/).

A Case Experience:

The Difference a Minute Makes

Melia Kelley

Standard disclosure:

This represents a targeted investigation, and not all portions of the exam will be discussed. Please don't take this as Standard Operating Procedure (SOP). Also, my set of tools has been evolving, but steps I mention should be able to be performed with a variety of different tools.

Tools:

EnCase v.6.18

RegRipper

PhotoRec

VMWare

Background:

Possible data spoliation:

The client requested an investigation that looked into data deletion on a Windows XP system within a specific time frame. The system in question had been in use for a couple of months after the time of interest. The end result was a report that detailed recovered files of interest and a timeline of events.

Investigation Plan:

Recycle bin analysis

File recovery using EnCase

File carving using PhotoRec

Analysis of carved files on system for context

Search for data deletion software

Registry and restore point analysis

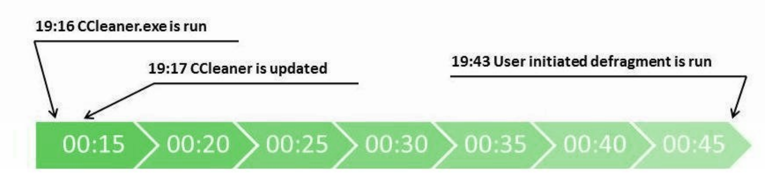
Timeline generation

Actual Investigation:

The scene: Me smoking a cigar in a shadowy room with my feet on the desk, looking debonair.

While recovering the deleted files was of great interest to the client, what makes this case stand out to me is what I found on the system regarding a program called CCleaner. Many of you are likely familiar with it, and have come across it in your cases (in fact, Cheeky4n6Monkey has some great posts about pulling artefacts relating to CCleaner using a RegRipper plugin) It seems to crop up an awful lot in certain types of cases. What made this one interesting was the reconstruction of events found in restore point registry hives. Luckily for me, though the computer had been in use for quite a while after the timeframe of interest, the restore points for the timeframe were still present.

I could see that the registry entries showed CCleaner being installed on the system a couple of years before the timeframe of interest. Even better, after tracking down RPs for specific dates, and determining the proper user, the keys showed that CCleaner.exe had been run on the system by the user in the "hot zone". Bingo! But wait... it wasn't quite as clear as that. You see, a good minute after CCleaner.exe was run, a CCleaner installer file called ccsetup###.exe was run, with no indications that CCleaner.exe was run again after the installation. So, was CCleaner simply updated but not run? Or could it have been run after the installer without updating the registry entry?


19:16 CCleaner.exe is run
19:17 CCleaner is updated
19:43 User initiated defragment is run
00:15
00:20
00:25
00:30
00:35
00:40
00:45

I had come across CCleaner enough in the past to know that the program will check for an updated version of the software and ask the user if they want to download it if one is available. So it didn't come as a surprise that an installer file would be run soon after executing the program. The question became, after running the installer, if CCleaner was run what changes, or lack of changes, would occur in the registry?

It was time to stop speculating, and start researching. I used a Windows XP machine that had CCleaner already installed. Upon firing up the program, I was indeed prompted to update the software. Following the update, I used the default option to start CCleaner automatically, and then ran the default CCleaner process on the system. Following the run, I examined the test registry hives to see what sort of information was present. The test system registry hives mimicked the investigated system: though CCleaner had been run following the updated installer file, the registry just reflected the initial execution of the program.

Moral of the Story

Now, I don't expect that this is an earth-shattering revelation. I guess the real point that I want to make is the importance of testing when questions are raised or anticipated. In this case, there were questions, and I had the ability to confidently say "I tested the process and the data is consistent." There are so many variables on systems, testing should be common place. You don't need a plethora of extra equipment to do it, either. Run some virtual machines, have a few baseline setups you can use, and take the time to experiment.

******* *This was previously published in the author's blog at : http://girlunallocated.blogspot.com/2012/02/case-experience.html*

Melia Kelley, is a seasoned Digital Investigator and is currently a Senior Forensic Consultant with First Advantage Litigation Consulting in the U.S.A. who has honed her skills working with the Military in Iraq. She is a well respected contributor to the Digital Forensics Investigation Blogosphere.

Virtual Forum Against Cybercrime

Issue: 09
Feb

Submitted Article

Gang Rape in the Assembly.

Debarati Halder

*** The author does not intend to hurt anybody's political sentiments. This is an independent view of the author and the author has expressed her views in her own right towards exercising freedom of speech. If anybody feels hurt, the author apologises in advance.*

As we curiously observed the legal battle over censorship between Google and a score of other websites and the Indian courts, we got a "nice" surprise. It was not from the Google, or from Facebook or even from any of the rest of those websites, neither from the courts or legal fraternity; but from three ministers in Karnataka state, which is known to have India's first and most famous cyber crime police cell.

While the assembly was being stormed by some very important debate, one of these ministers allegedly was looking at a clipping which involved sex, the abuse of woman, violence which was probably in violation of India's Internet decency codes.

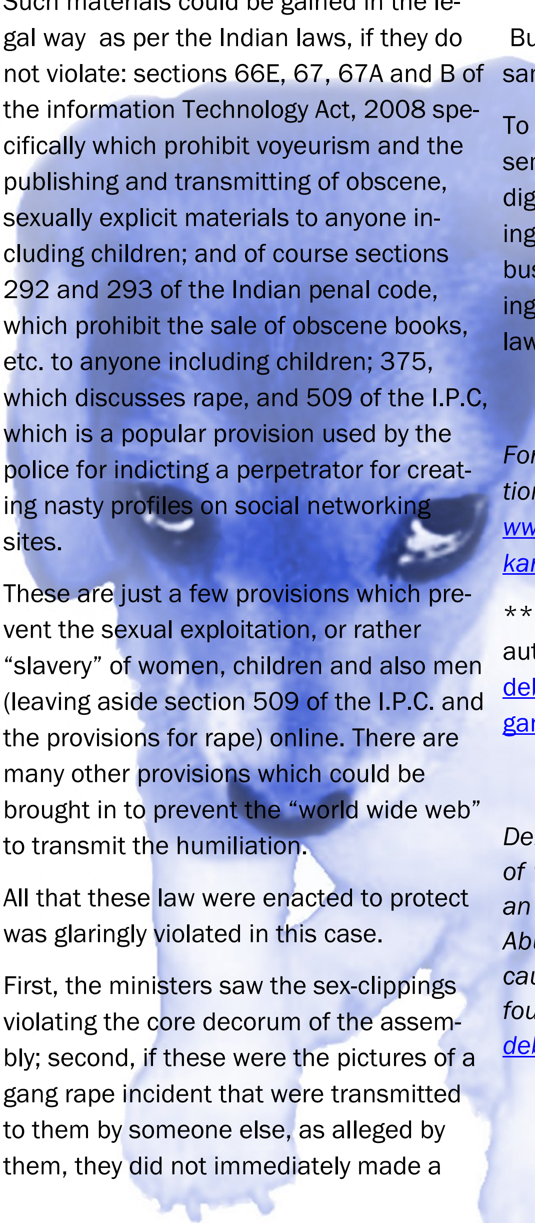
The news reports suggested that it was the minister for cooperation who had the mobile phone device placed between his lap and the desk and started watching the video. He then started "flipping through pictures of women".

The other two ministers joined him out of curiosity were the minister of ecology, environment and ports; the other was none other than the minister in charge of women and child welfare.

The ministers were immediately indicted and later voluntarily resigned from their posts. Even though they argued that they were seeing the clipping of a gang-rape incidence that was sent to the mobile phone device, their argument has yet to be proved.

But the issue that really moved me was, probably no human being can resist himself from viewing sex-related video images...but should they watch this stuff in the assembly? No way...

Viewing pornography isn't illegal under Indian law. Quite a long time ago the Bombay High court refused to provide a blanket ban on porn materials on the Internet. The high court rightly held that law cannot stop a person's sexual rights (including right to be aroused by viewing such materials), if these materials are gained in the legal way and seen in private.



Such materials could be gained in the legal way as per the Indian laws, if they do not violate: sections 66E, 67, 67A and B of the information Technology Act, 2008 specifically which prohibit voyeurism and the publishing and transmitting of obscene, sexually explicit materials to anyone including children; and of course sections 292 and 293 of the Indian penal code, which prohibit the sale of obscene books, etc. to anyone including children; 375, which discusses rape, and 509 of the I.P.C, which is a popular provision used by the police for indicting a perpetrator for creating nasty profiles on social networking sites.

These are just a few provisions which prevent the sexual exploitation, or rather "slavery" of women, children and also men (leaving aside section 509 of the I.P.C. and the provisions for rape) online. There are many other provisions which could be brought in to prevent the "world wide web" to transmit the humiliation.

All that these law were enacted to protect was glaringly violated in this case.

First, the ministers saw the sex-clippings violating the core decorum of the assembly; second, if these were the pictures of a gang rape incident that were transmitted to them by someone else, as alleged by them, they did not immediately made a note to the assembly, which they should have, especially since the minister for women and child development was involved; third, the clipping itself is shrouded in controversy, it may have also violated the legal provisions meant for Internet sex-offences as I mentioned above.

The ultimate result... a real gang rape of the laws meant to prevent sexual exploitation of women online. It is hoped that very soon the incident will be probed and the real story behind the hush-hash viewing of the clippings by the ministers will be revealed; probably they will positively testify their own argument.

But the underlying fact remains the same.....

To some, audio-visual clips of naked or semi-nude women, transmitted through digital technology are the most entertaining materials, even when compared to a busy and important commitment like making, breaking or deciding the fate of the laws in the parliament................. Shame......

For more information on the events mentioned in this story please see http://www.thehindu.com/news/states/karnataka/article2869723.ece).

*** This was previously published in the author's blog at http://debaraticyberspace.blogspot.in/2012/02/gang-raped-in-assembly.html

Debarati Halder is the Managing Director of the Centre for cyber victim counselling, an advocate for WHOA (Working to Halt Abuse online) and works tirelessly for the cause of women online. Her blog can be found at http://debaraticyberspace.blogspot.in/.