USE OF CYBER FORENSICS IN TRACKING CYBER CRIMES

Dr. Digambar Pawar
Associate Professor
University of Hyderabad
dpr@uohyd.ac.in
+91 9491463815
Today’s agenda

- Recent trends
- Cyber Crime
- Digital Evidence
- Digital Forensics
  - Search & Seizure
  - Authentication
  - Acquisition
  - Analysis &
  - Presentation and report
- Digital Forensic tools
- Email Tracing
- Discussion
CYBER CRIME
THE NAZIS ARE COMING, THE NAZIS ARE COMING!!

THE E-MAIL SERVER IS DOWN!!

TERROR IN THE 20TH CENTURY...

TERROR IN THE 21ST CENTURY...
What Happens in an Internet Minute?

- 204 million emails sent
- 47,000 app downloads
- $83,000 in sales
- 61,141 hours of music
- 20 million photo views
- 320+ new Twitter accounts
- 100,000 new tweets
- 20 million photo uploads
- 639,800 GB of global IP data transferred

And Future Growth is Staggering

Today, the number of networked devices = the global population
By 2015, the number of networked devices = 2x the global population
In 2015, it would take you 5 years
To view all video crossing IP networks each second
Morphing of Images
ఎమముందు లేపారు పిలువాలి!

సహిష్ణుతున్న సిద్ధాంతాన్ని పిలువాలి...
Viral images

This is NOT London, NOT Singapore

This is our GUJARAT, Cheers to Modi...

NO COMMENTS!
Myth Busted!

A simple image search on google brings me this image:

which clearly shows that this place is somewhere in China (see the green signs on the right-top, the bus-stop signs towards the left and right edges). Turns out, this is a photo of the BRT (bus rapid transport) in Guangzhou, China. Check out this article: http://thecityfix.com/blog/guangzhous-brt-revolutionizing-perceptions-of-bus-travel-in-china/.
Hacking

Student held for hacking into GTU website

Student changed data to get admission in MCA

PTI | June 5, 2010

A student has been arrested for allegedly hacking into the website of Gujarat Technological University (GTU) and changing its data to get admission in a post-graduation course, police said today.

Yogesh Patel, who hails from Jamnagar and has completed his Bachelor of Computer Application course (BCA), was arrested by Ahmedabad crime branch here last night, they said.

Patel had allegedly hacked into the GTU website for getting admission in Master of Computer Application (MCA).

Primary investigations revealed that Patel got an internet connection allegedly by submitting fake documents and was helped by four of his friends.

Patel has been taken to Ahmedabad for further questioning while efforts are on to nab his associates, police said.

The arrest was made following a complaint lodged by GTU in Ahmedabad.
Thiruvananthapuram airport’s website, which was hacked, restored now

Calling themselves 'Kashmiri Cheetahs', the group was responsible for the hacking of AIIMS Raipur's website earlier this year.

In what seemed to be another case of cyber crime, the official website of Thiruvananthapuram airport was hacked by a group which claims to be from Pakistan earlier Wednesday. The recent cyber attack comes following several events of hacking of Indian websites by Pakistani groups. However, thirty minutes after it was hacked, the website was found to be restored to its original form.
Cyber attacks: Mallu Cyber Soldiers hack Pak website

DECCAN CHRONICLE | ROHIT RAJ
Published Jan 19, 2017, 7:23 am IST Updated Jan 19, 2017, 7:36 am IST

EXTERNAL PUBLICITY WING
Ministry of Information, Broadcasting & National Heritage (IB & NH)
Government of Pakistan

World recognizes Pakistan's role in regional peace, stability: Fatemi
Govt to provide natural gas to maximum masses: Saqib
Govt focused on improving key macroeconomic indicators: Dar
Zardari h
I. M. STEWPEED: UPSC website hacked with Doraemon image, title song plays in background

Sep 11, 2018, 10:51 AM IST
Cyber Bulling

- “Willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices” OR
- “The use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature”

- Children may be reluctant to admit to being the victims of cyber bullying
- Examples:
  - Someone repeatedly makes fun of another person online
  - Repeatedly picks on another person through e-mail or text message
  - When someone posts something online about another person that they don’t like
Cyber Bulling (contd..)

Woman stands up to cyber blackmailer with a brave Facebook post

US-based Indian woman takes on cyber bully with a gutsy public post; receives support in her endeavour.

Subject: LONG TIME NO SEEN TARUNA ASWANI. Does that look familiar and more I got.
To: *taruna.aswani@gmail.com*
Cc: 

Hello there, it has been long since I saw you in Mumbai and I found out you went out of the country. I used my computer skills to trace you through your friends and social media and I found you. I have nude pictures and video that belongs to you that nobody else knows it exists beside the person you sent to and it looks good like I thought. All I am saying is if you want me to keep quiet on this and don't let the world(social media, Work place, family and friends) know then you have to excite me. Let me masturbate like you did in that video. I will give you 24 hrs to respond and 48hrs to send me and after that you might be famous if you act smart.

So you know I have plan B because I expect you to smart as per your past history and try go to police go ahead ... oops I am 1000's of miles away but still I wanted to give you a chance. You can try your best and do that. This is not a treat but if I ask you nicely you won't do it, we might as well be both happy that this remains the way it is or be sad and live with it.

You know what I have. You in the bathroom with your blue Sandles. I have access to your all your friends/social media and family and co-workers(NMS healthcare and heritage inc) contacts that you have and I think some will be happy and some embarrassed to see it but if you have a thick skin then it shouldn't worry you. All I want is pics of your pussy opened with your fingers and a small clip, you don't have to include face I will know if it's you or not and I like it shaved!

As embarrassing as the videos may be (they were sent to my boyfriend at the time) I choose to stand up to this man. Instead of cowering down to his requests. I do this so that other women may take a lesson to stand up to bullies and low life's like this and may get the confidence to stand up as well in case he is known to us and is targeting all of us, but we're either too scared, ashamed or clueless in how to manage or handle such situations.

I implore you to share this post with as many people as you know to get the word out. Perhaps someone may be able to locate this person through his digital footprint.

Please help me in nabbing this sick pervert.

If you find any information on this, please inbox me so I can report it to the Detective working on the case or you may contact him directly on +1 301 699 2601 and mention my name for reference.

Grateful for your help in this, I have enclosed along with this screen shots of his emails- I have deleted the photos/videos he had attached.

Thanks for all your help and support in this.

Yours truly,

Taruna
Cyber Crime

“Unlawful act wherein the computer is either a tool or a target or both”

Two aspects:

- Computer as a tool to commit crime
  - Child porn, threatening email, assuming someone’s identity, sexual harassment, defamation, spam, phishing, etc.

- Computer itself becomes target of crime
  - Viruses, worms, software piracy, hacking, etc.
Cyber Crimes (contd..)

- Hacking
- Identity Theft
- Cyber Bulling
- Pornography, Child Pornography
- Data Theft
- Spreading Virus & Worm
- Phishing
- Disruption of Computer/Network
- DOS Attack
- Cyber Terrorism
- Email Fraud
- Email Spoofing
- Credit Card Fraud
- Copyright Violation
- Web Defacement, etc.
Why Digital Evidence?

We need a means for investigation & analysis of the crimes – to bring the culprits to conviction.

All solution lies in Digital Evidence
Digital Evidence

 Definition

Digital data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator.

 Categories

– Text
– Audio
– Image
– Video
DIGITAL FORENSIC
Cyber Forensics

Cyber Forensics deals with forensic analysis of cyber crimes with the objectives of

- Identifying digital evidence
- Acquiring digital evidence
- Authenticating digital evidence
- Analyzing digital evidence
- Reporting digital evidence

Role of Cyber Forensics

A means of systematically gathering digital evidence, analyzing it to make credible evidence, authentically presenting it to the court of law.
Cyber Forensics-Steps

Preservation → Presentation → Analysis → Authentication → Acquisition → Seizure & Hashing → Identification → Scene of Crime → Forensics Lab

Preservation
Presentation
Analysis
Authentication
Acquisition
Seizure & Hashing
Identification
Scene of Crime
Forensics Lab
Cyber Forensics :: Classification

Cyber forensics

- Traditional Forensics
- Live Forensics

Source?

- Disk Forensics
- Cloud Forensics
- Device Forensics
Hashing

- Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string.
- Different hash values imply different contents.
- Identical hashes (strongly) suggest identical contents.
- Verify integrity of evidence.
- Automatically identify known content during an investigation.
- Examples... MD5, SHA, etc.
Hashing

Test.doc

Hang him not, kill him

Hasher (MD5)

00F0C7E92A1847548C006C180165DFB1

Message Digest

Test.doc

After modification

Hang him, not kill him

Message Digest

6FB3938D0271301C6C4AC847908AB26D
Hashing

CyberCheck - Hasher 1.0

- Flat image
- TrueBack Image

File Name
Browse...

- MD5
- SHA-1
- HMAC

Key (Max.12 chars) :
Message Digest :
Time Taken :

Exit
Acquisition

- The process of making a bit stream image of the digital evidence.
- Acquisition is always done in a trusted write blocked environment.
- Acquisition of Evidence is normally done after the process of seizure.
- Acquisition needs a higher capacity destination than the Source
Acquisition tools

- TrueBack
- FTK imager
- EnCase Forensic Imager
- dd imager, etc.
Acquisition
Analysis

Process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence.

- **REMEMBER** ANALYSIS SHOULD BE REPEATABLE
Analysis (Cont..)

- Forensic analysis can reveal:
  - what web sites have been visited?
  - what files have been downloaded?
  - when files were last accessed?
  - attempts to conceal or destroy evidence?
  - attempts to fabricate evidence?
  - and many more...
Analysis (Cont..)

➤ Should look into
  • Slack Spaces / lost clusters / protected data area / protected files / steganographic contents / encrypted files/ unallocated area / Swap area

➤ Should do
  • Format recovery
  • Partition recovery
Analysis (Cont..)

- **Hiding data**
  - Renaming files
  - Changing file extensions
  - Turning on hidden attribute
  - Concealing information in a part of the disk where data would not normally exist
  - Hiding using ADS, etc.

- Identify these hidden data
Analysis (Cont..)

➢ Tools

- Encase
- FTK
- CyberCheck
- Oxygen Forensic Suite

- TSK
- DFF, etc.
Analysis
Analysis
Email Tracing
Send Anonymous Email

Every day over 60,000 free anonymous emails are sent from our servers, making us the world's largest and most trusted anonymous email service.

This service is perfect for the following

- catch a cheating spouse husband or wife.
- find out if your friend is a real friend
- give warnings to people
- inform the police about illegal activities
- inform the tax office about tax cheaters
- confess your love to somebody
- play an email joke with your friends
- when your own email service doesn't work
- if your private email is banned by the recipient
- report fraud to your boss or institution
- and many more reasons...

Note: By sending a fake email or prank email you may be committing the offence of fraud even you did not intend to. You are not allowed to use this service for any illegal activities at any time.

SendAnonymousMail is not liable for your emails you send at any time. Try not to do anything stupid or you might end up needing a divorce.

Don't do anything illegal. If you send death threats, abuse, slander or anything illegal we WILL publish your IP address and block you from this site.

Abusers can be reported here.

Receiver's email: paward1980@gmail.com

Sender's email: principal@glendaleacadem

Subject: Student report for the month

Dear Parents,
Congratulations to you and your ward for achieving A+ grade in the grand final.

Yours Sincerely,
Principal, GA

unbadhar

By pressing "SEND" you accept our terms and conditions and accept that your email contains no illegal, abusing, harrassing or likewise content.
Conclusion

• Many computational platforms are evolving which lacks the support for crime investigation in terms of the required frameworks/tools

• Need to be Self Reliant. Make In India and Digital India are opportunities for us to emerge with indigenous solutions and products for Digital Forensics (specially for cloud, IOT, etc.)

• Take major initiatives for educating and making people aware of the dangers and the ways to mitigate them

• Launch programmes and schemes to increase the number of cyber security experts in the country

• Establish strong Public-Private links

• “Monitoring of Critical Infrastructure Systems” is always a challenge!
Discussion
Thank You