



February 2019

Cybersecurity and Forensics

PWC G8 Gals@Technology



"I'm the oldest employee in the store...
I've been here from Hi-Fi to WiFi."

Current Topics

- Wi-Fi Branding is confusing – 802.11a, b, g, n, ac,
 - ALL Wi-Fi is licensed in the 2.4GHz and 5GHz radio frequency band
 - Difference is speed – 11Mbps to 3.46Gbps
 - New naming is Wi-Fi 1 thru Wi-Fi 6
 - Currently most popular is Wi-Fi 4 (aka 802.11n, max 600Mbps)
 - 2019 products will be Wi-Fi 6 (aka 802.11ax, max 10.53Gbps)
 - Looks for numbering on routers and Wi-Fi devices

BLUETOOTH VERSIONS

Here's a quick summary to explain the commonly encountered Bluetooth versions and the differences between each grade.

Bluetooth Versions	Optional Features					Bluetooth Version description
	Basic rate (BR)	Enhanced Data Rate (EDR)	High Speed (HS)	Low Energy (LE)	Slot Availability Masking (SAM)	<p>Note: The additional features supported by the higher versions of Bluetooth are all optional and do not affect the encoding and transmission of audio. Higher versions of Bluetooth are also backward compatible and will default to the available features of that Bluetooth connection.</p>
Bluetooth 1.x	Yes	No	No	No	No	<p>The basic Bluetooth rate with no additional/optional profiles or codecs. This version of Bluetooth is obsolete and was rarely implemented on mobile devices due to its limited speed of 1mbps and difficulty pairing.</p>
Bluetooth 2.x	Yes	Yes	No	No	No	<p>The most popular variant of Bluetooth, especially in the earlier days when phones were not as advanced. It supports enhanced data rates (EDR) up to 3 Mbps, and the V2.1 variant significantly simplified the pairing procedure making it a more practical for commercial use.</p>
Bluetooth 3.x	Yes	Yes	Yes	No	No	<p>Bluetooth 3.0 improves on the speed limitations of Bluetooth 2.1, with the optional High-Speed feature (HS), which allows the Bluetooth module to transmit over an adjacent radio (802.11). However, Bluetooth 3.0 consumes a lot more power than Bluetooth 2.x.</p>
Bluetooth 4.x	Yes	Yes	Yes	Yes	No	<p>Bluetooth 4.0 has the high-speed capability of Bluetooth 3.0 but also comes with a Low Energy feature to collect data from the sensors of low rate devices. This feature allows the Bluetooth module to reduce power consumption with connected devices like wearable smartwatches, heart monitors, mobile phones and smart headphones.</p>
Bluetooth 5.x	Yes	Yes	Yes	Yes	Yes	<p>The most recent iteration of Bluetooth, better suited for the Internet of Things (IoT). It's speculated to have twice the bandwidth of Bluetooth 4.2 LE and 4x the range. It also has a new feature called Slot Availability Masking (SAM) which can detect and prevent interference on neighboring bands for a more efficient use of broadcasting channels. However, we have yet to test the Bluetooth 5.0's capabilities for ourselves.</p>

Current Topics

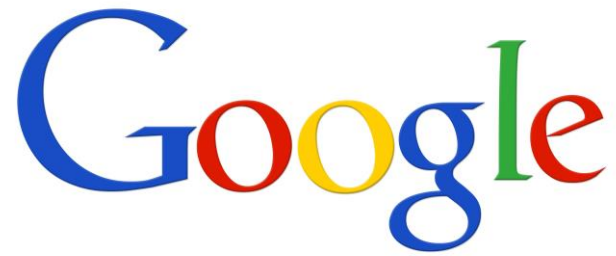
- Cybersecurity problems with Government shutdowns
 - Expired software licenses and encryption certs
 - Weeks-worth of unanalyzed network logs
 - Activity increased from China, Iran, North Korea, and Russia
 - Security employees are difficult to find. This just made it more difficult.
 - Only Silver Lining – furloughed employees weren't clicking on spear phishing emails





Current Topics

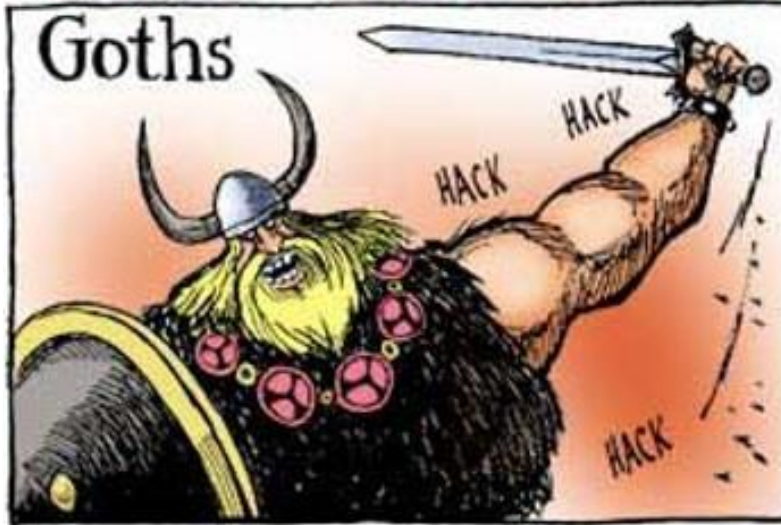
- Massive breach leaks 773 million email addresses and 21 million passwords
 - 87 gigabytes of data known as “Collection #1”
 - Represents years of data (since at least 2008) from 2,000 different sources
 - Demonstrates the risk of using old passwords with new accounts on different platforms. The “dictionary of passwords” is out there.



Current Topics

- Google Chrome announces extension to check for stolen passwords
 - Only checks username/password combinations
 - Developed with crypto experts at Stanford to ensure Google *never* learns your username/password
 - Based on internal Google database containing over 4 billion username/password from public sources of previous breaches
 - Similar but more conservative/secure than “Have I Been Pwned” service

BRINGING CIVILIZATION TO ITS KNEES...



There should be a law

- Indiana Computer Tampering, IC 35-43-2-3
- Indiana Computer Trespass, IC 35-43-1-4

- Computer Fraud and Abuse Act, 18 USC 1030
- Wiretap Act, 18 USC 2511
- Electronic Communications Privacy Act, 18 USC 2701



There should be a law ...

- Child Pornography, 18 USC 2252A
- Criminal Copyrights, 18 USC 2319 & 17 USC 506(a)
- Criminal Trademark, 18 USC 2320
- Criminal Trade Secrets, 18 USC 1831, 1832
- Treats and Harassment, 18 USC 844(e) & 875, 47 USC 223(a)(1)(C, E)
- Fraud, drug dealing, other, etc.



“The Computer” and “The Network”

- Computer as **Target** of the incident
 - Get to instructor’s test preparation
 - Access someone else’s homework
 - Access/Change a grade
 - Access financial information
 - “Denial of Service”
- Computer as **Tool** of the incident
 - Word processing used to create plagiarized work
 - E-mail sent as threat or harassment
 - Printing used to create counterfeit material
- Computer as **Incidental** to the incident (a **Witness**)
 - E-mail/file access used to establish date/timelines
 - Stored names and addresses of contacts or others potentially involved in the incident



Dr. Edmond Locard

- French criminalist born in 1877
- Considered the godfather of modern-day forensics
- Locard's Exchange Principle

“Every contact leaves a trace”



"Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value."

Crime investigation: physical evidence and the police laboratory.
Interscience Publishers, Inc.: New York, 1953

You have seen this in Pop Culture

- Locard's principle is mentioned in the sixteenth episode of CSI: Crime Scene Investigation, "Too Tough to Die", aired on 1 March 2001.[20]
- "Locard's Exchange" is the title of episode#75 of the television medical drama Crossing Jordan, aired on 10 April 2005.
- "Locard's exchange principle" is mentioned near the end of chapter 17 in the novel "Break No Bones" by Kathy Reichs.
- "The Locard exchange principle" is mentioned in the Jemima Shore novel, "Cool Repentance", by Antonia Fraser.
- "The Locard exchange principle" is mentioned in the novel The Bone Collector, by Jeffery Deaver.
- "The Locard exchange principle" is mentioned in the novel I Am Pilgrim, by Terry Hayes.
- "The Locard exchange principle" is described as "transference" in the 2002 film, Murder by Numbers.
- The exchange principle is mentioned while Dexter is examining Cassie's body in an episode of the final season of Dexter. S08 E08 'Are We There Yet?'
- "The Locard exchange principle" is mentioned in the final episode of 2018 drama, Queen of Mystery 2.
- "Locard's exchange principle" is mentioned in season 1, episode 12 of the detective drama Day and Night.
- And many more

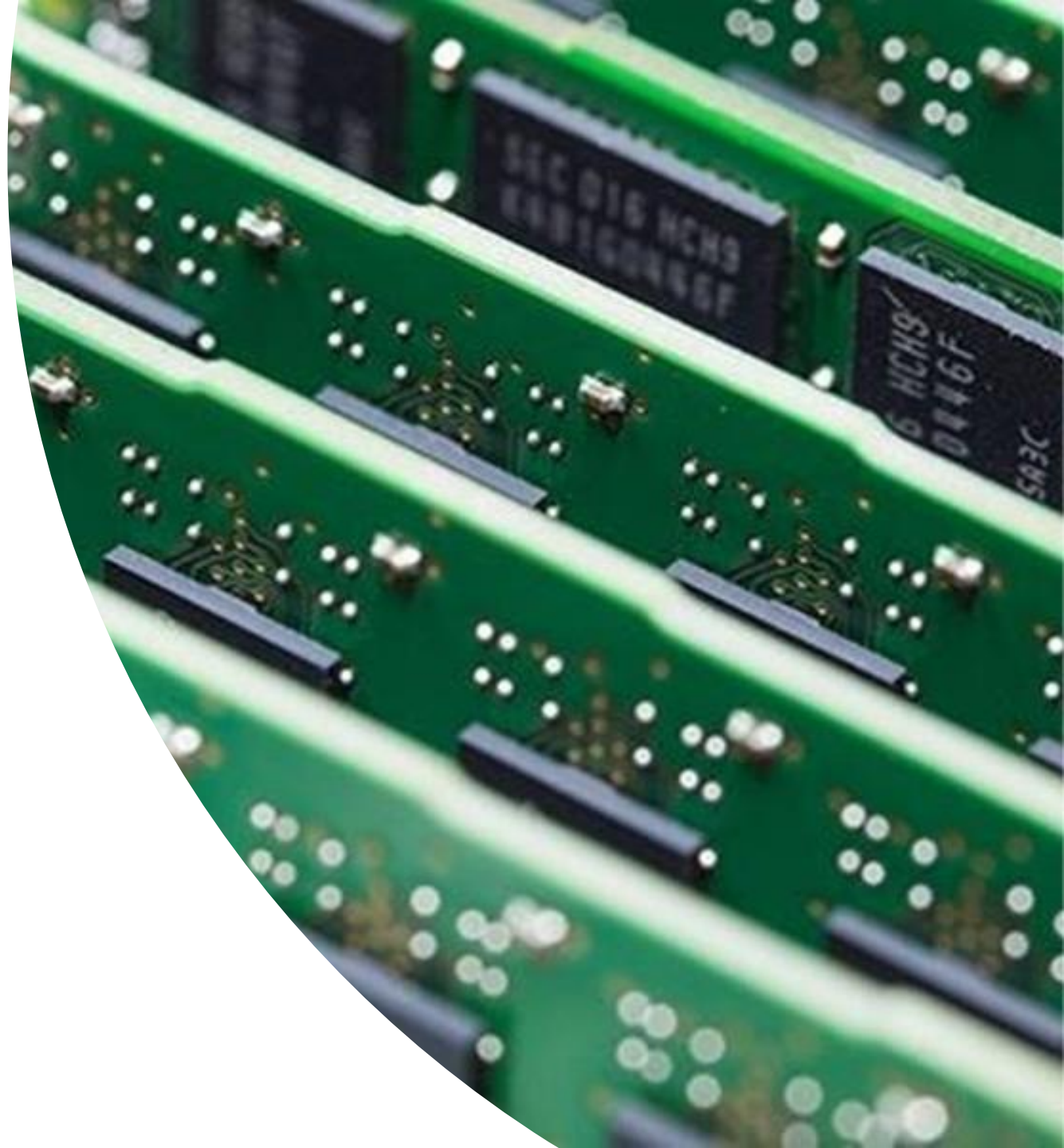
The Objectives of a Forensic Examination



- Conduct a **repeatable** and **verifiable** examination of “*the computer*” using established practices and procedures
- Successfully communicate results of the examination to the “trier of fact”
- Examiner must be a “teacher” as well as witness
- Maturing from “black art” to “science”

Basic Methodology

- The Three A's
 - **Acquire**
 - **Authenticate**
 - **Analyze**

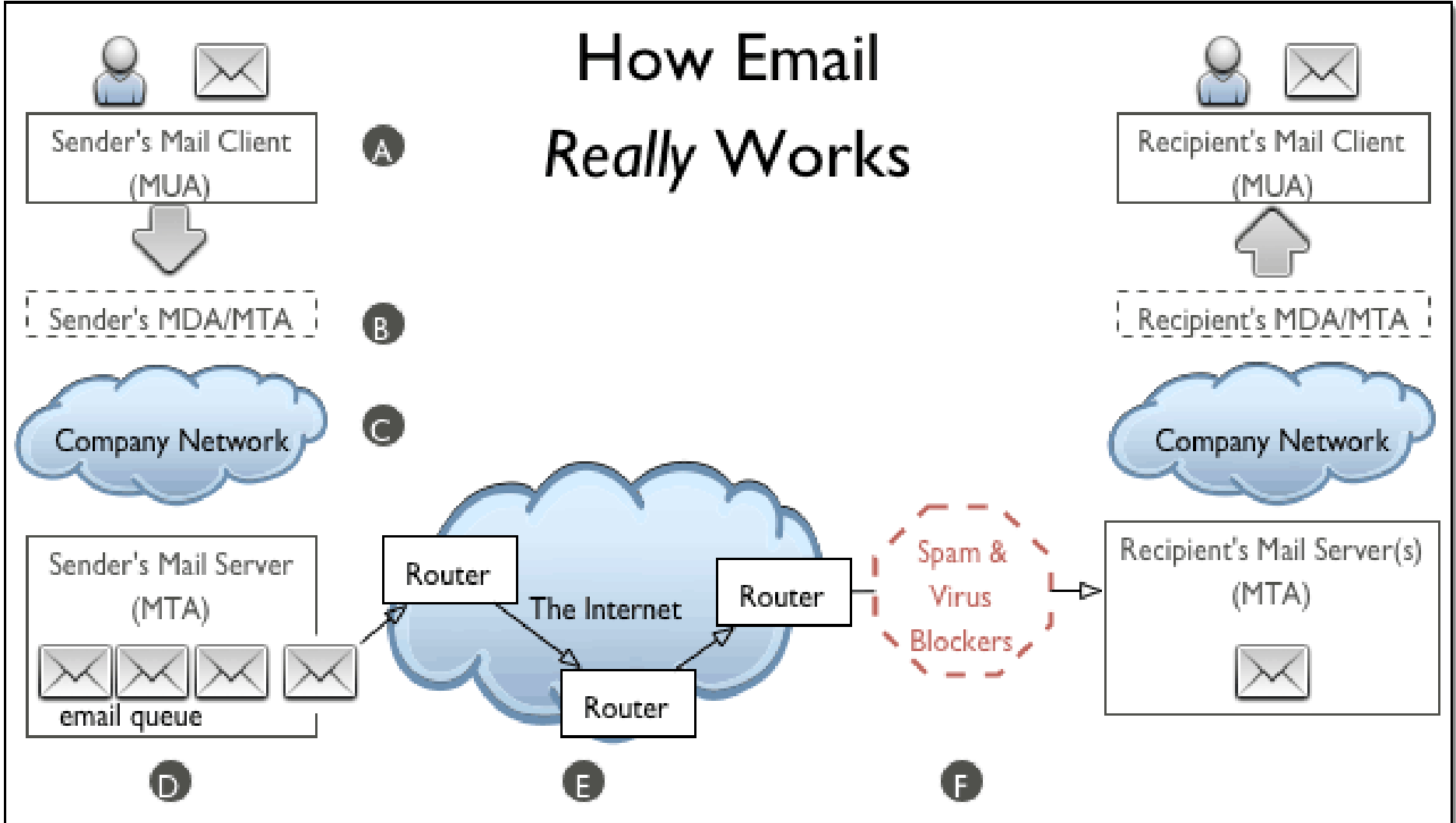




General Types of Digital Forensics

- “Network” Analysis
 - Communication analysis
 - Log analysis
 - Path tracing
- Media Analysis
 - Disk imaging
 - MAC time analysis (Modify, Access, Create)
 - Content analysis
 - Slack space analysis
 - Steganography
- Code Analysis
 - Reverse engineering
 - Malicious code review
 - Exploit Review

The “puzzle” is a combination of all the above pieces




North Korean Programmer Behind WannaCry

- Worldwide outbreaks 2015-2018
- DOJ indictment on September 6, 2018 was the largest of its kind in term of digital evidence
- Multi-national forensic effort





PARK JIN HYOK



business2008it@gmail.com
ttykim1018@gmail.com
pkj0615710@hotmail.com
surigaemind@hotmail.com

"Kim Hyon Woo" Alias Accounts

hyon_u@hotmail.com
Twitter @hyon_u
tty198410@gmail.com
hyonwu@gmail.com
hyonwoo01@gmail.com
mrkimjin123@gmail.com

xiake722@gmail.com
"Kim HyonWoo"
diver jacker@gmail.com
iaohu1985@gmail.com
"Kim HyonWoo"
Brambul Worm Collector Email Accounts

Operational Attack Infrastructure

Compromised Web Server

- mogbe123456@gmail.com
- "John Mogabe" Facebook
- hwa5403 DDNS account
- hwa5403@daum.net
- campbelldavid793@gmail.com
- goo19874@gmail.com
- [KB NAME REDACTED]@gmail.com
- [BM NAME REDACTED]@gmail.com
- amazonriver1990@gmail.com

- yardgen@gmail.com
- jasmuttly@hanmail.net
- "Andoson David" Facebook
- goffman_david2@aol.com
- Twitter @erica_333u
- bangsong8519@daum.net
- [FC NAME REDACTED]@gmail.com
- [MP NAME REDACTED]@gmail.com
- uiwon0608@daum.net

- watsonhenny@gmail.com
- "Watson Henny" Facebook
- rsaflam8808@gmail.com
- [MONIKER 3 REDACTED]@gmail.com
- stevegell77@gmail.com
- [SW NAME REDACTED]@gmail.com
- [LB NAME REDACTED]@gmail.com
- [JK NAME REDACTED]@gmail.com
- [KK NAME REDACTED]@gmail.com

- "WatsonHenny" LinkedIn
- MrDavid0818@gmail.com
- MrDavid0818@gmail.com LinkedIn
- agens316@gmail.com Facebook
- agens316@gmail.com
- jongdada02@gmail.com
- skyfriend202@gmail.com
- [JK NAME REDACTED]@outlook.com
- messilione1.messi2015@yandex.com

- jonnie.jemison@gmail.com
- changtony1989@hanmail.net
- Moniker 2 Facebook
- Moniker 1 Facebook
- [DJ NAME REDACTED]@gmail.com
- [JB NAME REDACTED]@gmail.com
- [ER NAME REDACTED]@gmail.com
- [JC NAME REDACTED]@gmail.com
- [JK NAME REDACTED] Facebook
- jamesmartin20162016@gmail.com

Alias Accounts

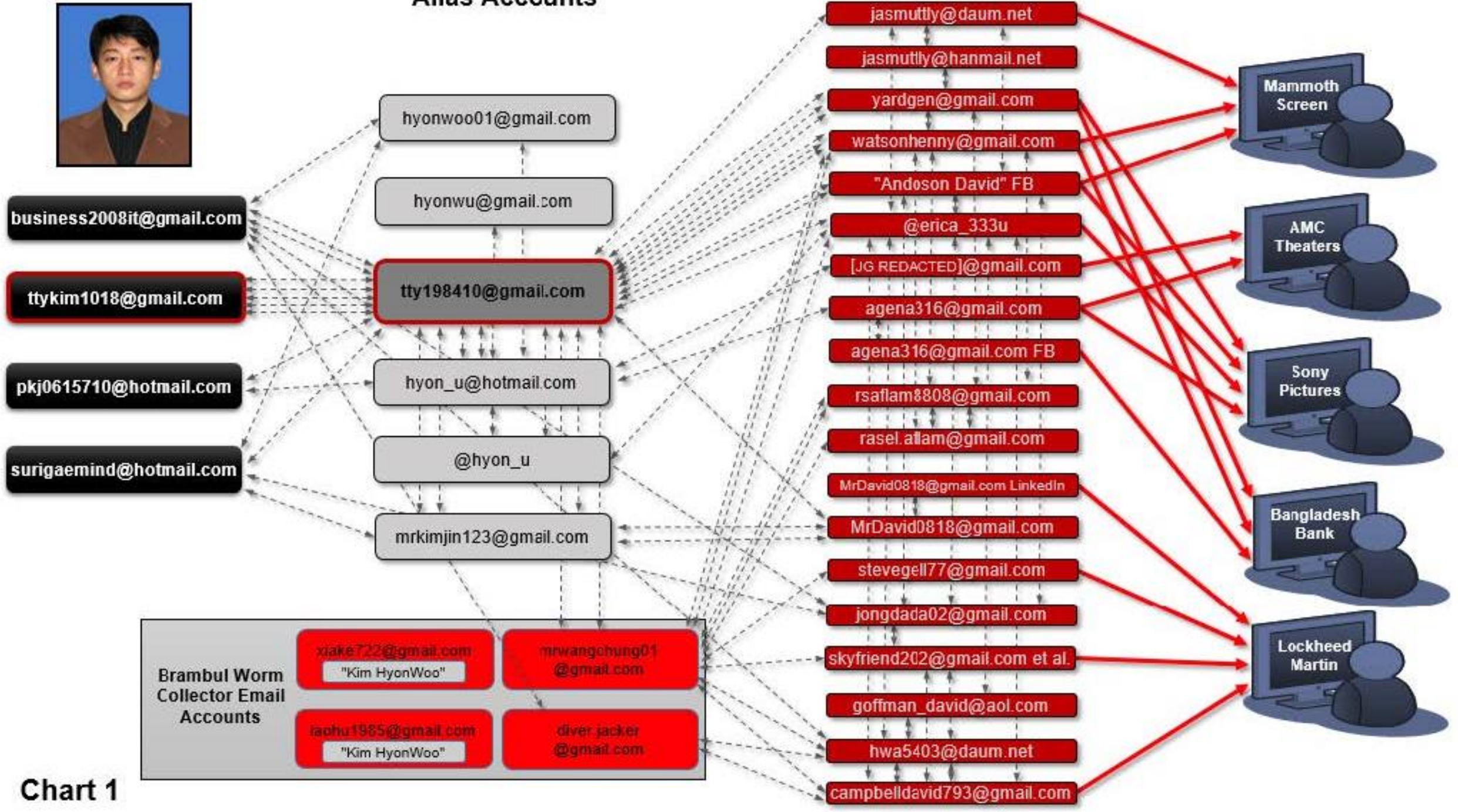


Chart 1

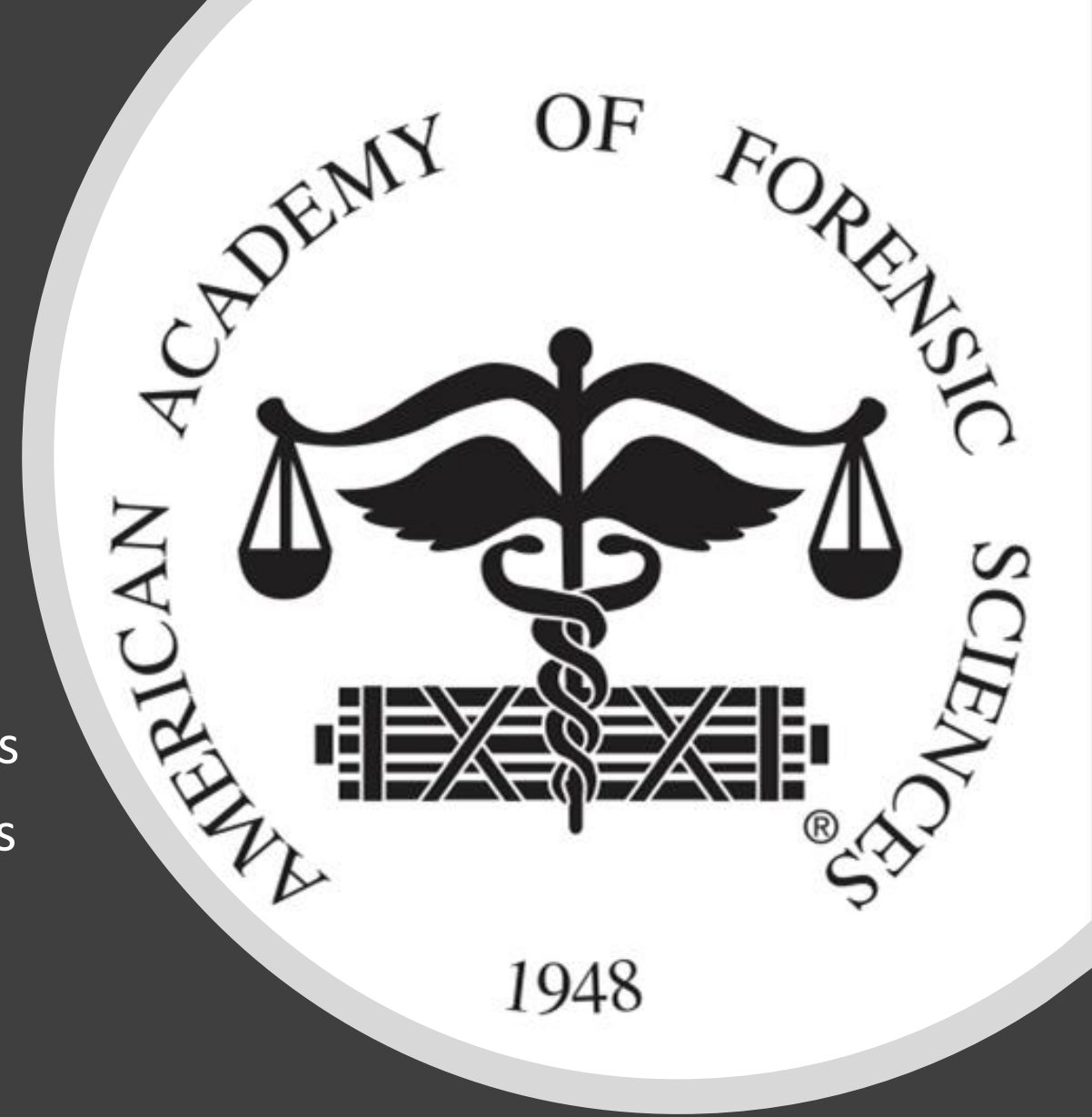


General Defense Strategies

- Not Me Defense (aka SODDI, TODDI)
- Mind-Numbing Detail Defense
- Indict the Examiner Defense (aka Dennis Fung Defense)

American Academy of Forensic Sciences

- Digital and Multimedia Sciences section established in 2010
- First new section in the Academy in over 50 years
- Three Purdue members in the initial 16 members
- Section now has 127 members



Computer Forensics

Some Personal “Firsts”

- First meeting with Doc Avolt in early-90s regarding student death with digital suicide note
- First meeting with Chief Cox in mid-90s regarding WL death with computer system next to bathtub
- First murder case in 2001 regarding murder of two Purdue students in Purdue village
- First international case in 2005 regarding murder in Lafayette with body found in Illinois and suspect arrested and charged in China
- First Federal Court experience with 2006 case of Purdue student making threats against the US President and his family
- First time pretending to be an 18-year-old girl for chat with possible sexual attacker
- More porn and abuse cases than I care to remember



Challenges Ahead

- The volume of data and the time to examine
- Worldwide legal issues
- The challenge of encryption
- Training examiners and the cost of staying current
- Cloud forensics



The 5th Wave

By Rich Tennant

© RICH TENNANT



"I've been an expert computer witness for over 20 years. I've testified about fraudulent whatnots, failed doohickies, missing thingys, you name it."