Digital Forensic Science: Ideas, Gaps and the Future

Dr. Joshua I. James
Joshua@cybercrimetech.com
2015-08-09

Overview

- Digital Forensic Science – where are we now?
  - Past
  - Present
- Where are we going?
  - Future
- What do we need?
- Thoughts on the (cyber)security of Korea

The Past.

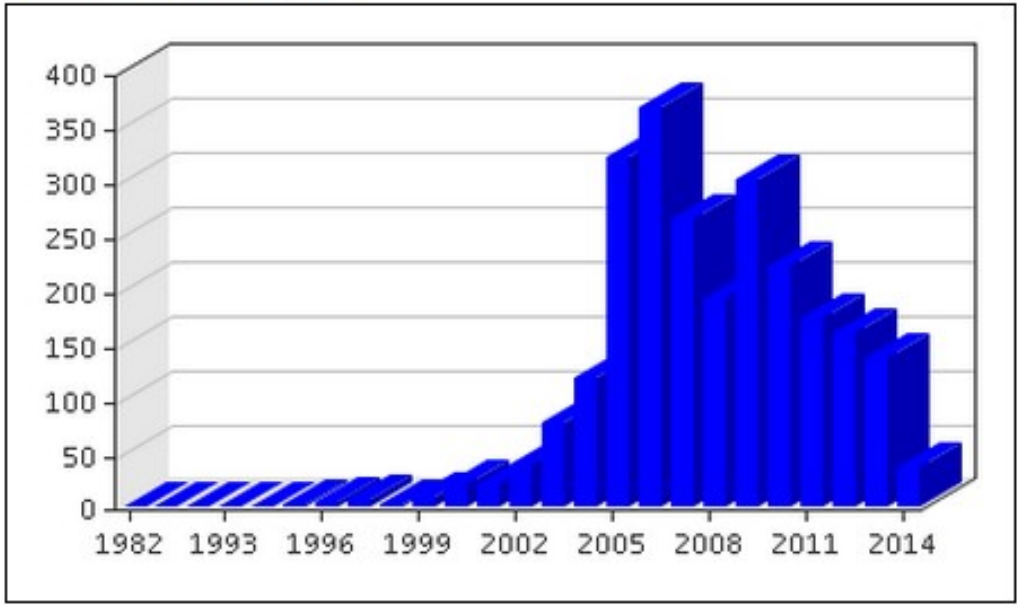
The Past: a review

- Electronic evidence started being more accepted in courts in early 1980s (mostly corporate & finance investigations)
- 1982 TCP/IP standard protocol for ARPANET
- The basis of digital forensics practiced by FBI in late 1980s
- Early 1990s – the Internet
- 1997 (Korea) Computer crime investigation team created
- 2001 (DFRWS) 'Digital Forensic Science' defined
- (Korea) Cyber Terror Response Center created
- 2003 Information security education rare, Digital Forensics education only at research (PhD) level
- 2005 Korea Digital Forensic Society (KDFS) created
- 2005 First billion Internet users

The Past: a review

Korea University CIST (usually DF-related) research output

Published items by year



Bibliometrics: publication history

Switch to overall percentile

Publication years	1982-2015
Publication count	2,682
Citation Count	11,461
Available for download	748
Downloads (6 Weeks)	2,984
Downloads (12 Months)	22,513
Downloads (cumulative)	206,626
Average downloads per article	276.24
Average citations per article	4.27

The Past: a review

- 2006 Digital Forensic Master's programs start opening in U.S. and Europe
- 2009 – Suspected NK cyber attack
- 2010 second billion Internet users
- 2010 - Stuxnet
- 2010's Increase in Korean IS programs – especially hacking / security
- 2011 – Suspected NK cyber attack
- 2012 KITRI BoB IS Program starts
- 2013 – Darkseoul
- 2014 DFRWS EU starts
- 2014 third billion Internet users
- 2014 CTRC becomes Cyber Bureau
- 2015 – Suspected NK cyber attack (hydro)
- 2015 Korea wins DEFCON
- 2015 ICDF2C comes to Korea (October)

The Past: Some problems

- 2010 Cybercrime costs estimated at $1 trillion
- 2011 - $114 billion
- 2012 - $110 billion
- 2013 - $100 billion
- 2014 - $445 billion
- 2015 - $445 billion to $2 trillion
- 2016 – Just pick a number…
- **Problems:**
  - We have short memories
  - We are horrible at measurement

The Past: Digital Forensic Research

- 2001/2002 – Standards, OS forensics, mobile devices, data reduction, attribution, encryption
- 2003 – DF Theory, OS forensics, mobile, data reduction, attribution, encryption
- 2004 – Frameworks, Processes, Process and Tool testing, OS forensics, attribution, where DF 'fits'
- 2005 – Data reduction, law, OS forensics, analysis techniques
- 2006 – memory, os forensics, law, fameworks, data reduction, verification, analysis techniques, fuzzy hashing
- 2007 – memory, data reduction, os forensics, automation
- 2008 – os forensics, memory, tool frameworks

Estimations based on prior DFRWS conferences and author experience

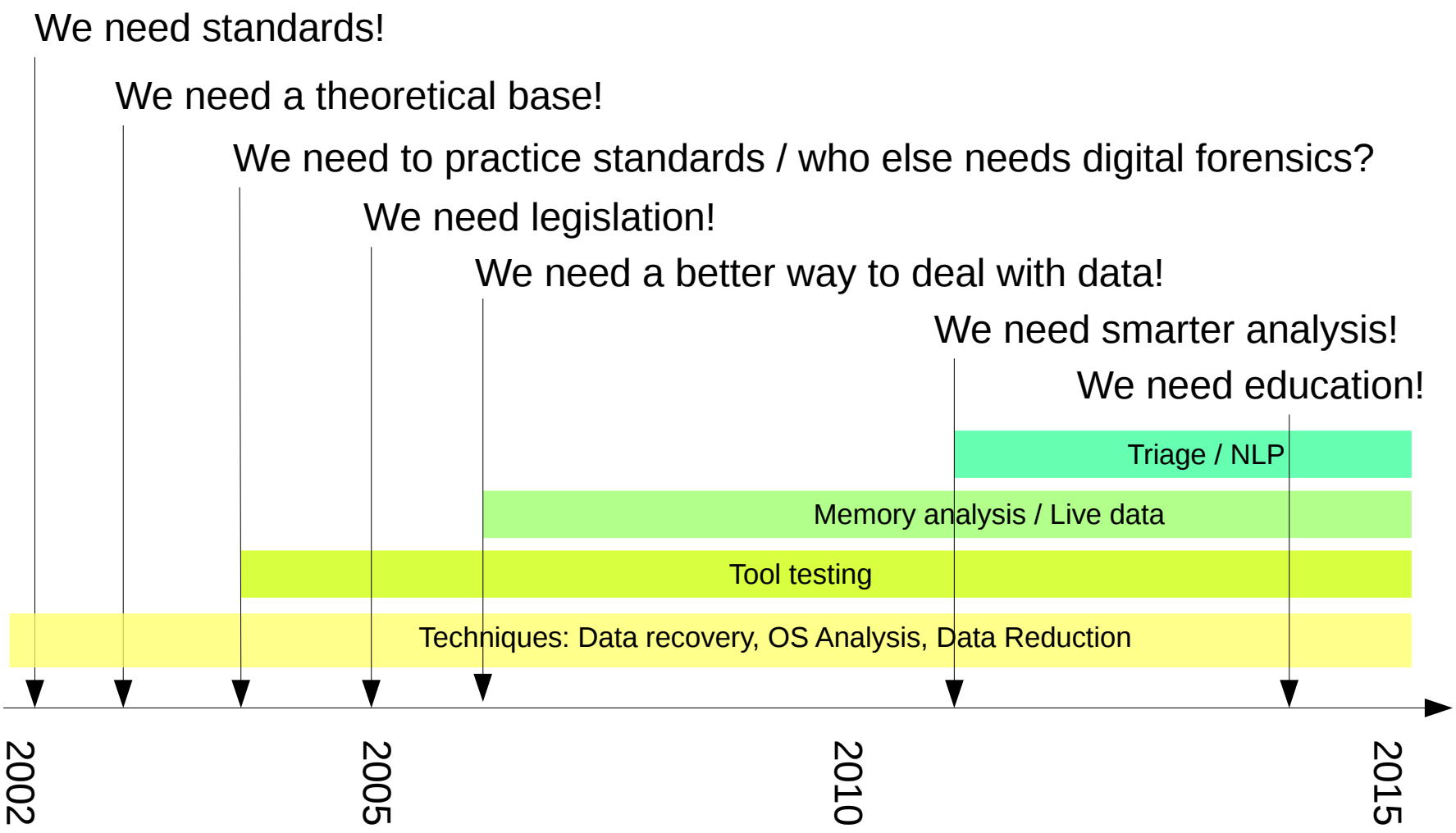
The Past: Digital Forensic Research

- 2009 – tool testing, data reduction, analysis, verification, os forensics, memory
- 2010 – os forensics, memory, mobile, verification, tool testing
- 2011 – verification, tool testing, law, analysis , live data
- 2012 – memory, language processing, analysis, data reduction, os forensics, fuzzy hashing
- 2013 – mobile, language processing, os forensics, fuzzy hashing, memory
- 2014 – memory, os forensics, DF education, non-traditional devices, data mining
- 2015 – malware analysis, data reduction, analysis, mobile devices, reverse engineering

Estimations based on prior DFRWS conferences and author experience

The Past: Digital Forensic Research

A very rough estimation



Estimations based on prior DFRWS conferences and author experience

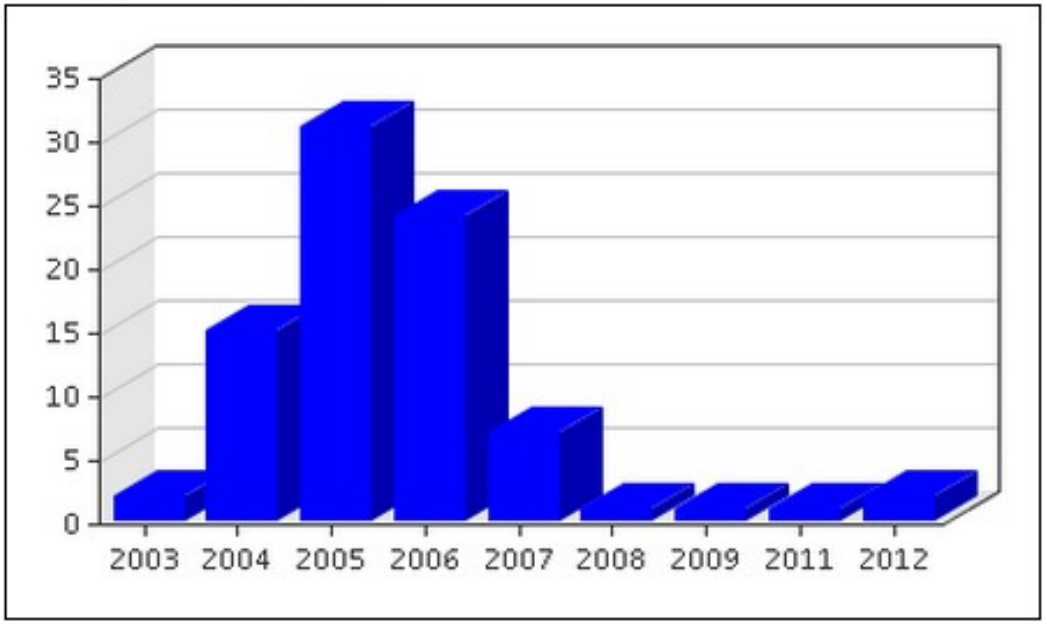
Where are we now?

The present

지금 : NSR Public Research (in English)

National Security Research Institute, Korea

Published items by year



Bibliometrics: publication history

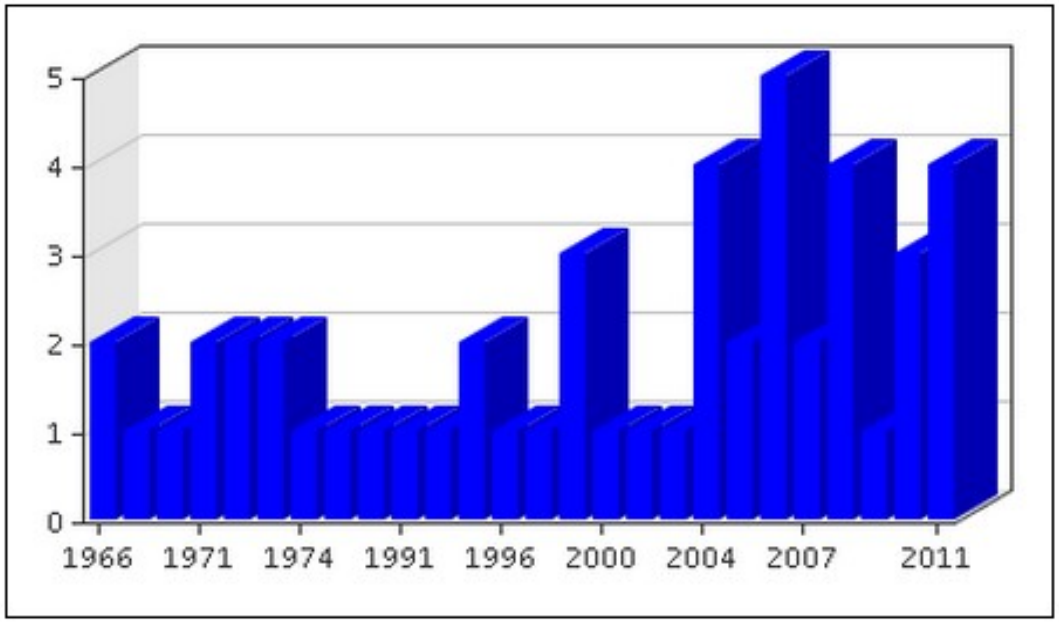
Switch to overall percentile

Publication years	2003-2012
Publication count	84
Citation Count	340
Available for download	7
Downloads (6 Weeks)	24
Downloads (12 Months)	259
Downloads (cumulative)	6,488
Average downloads per article	926.86
Average citations per article	4.05

지금 : NSA Public Research (in English)

National Security Agency, U.S.A.

Published items by year



Bibliometrics: publication history

Switch to overall percentile

Publication years	1966-2015
Publication count	52
Citation Count	351
Available for download	29
Downloads (6 Weeks)	172
Downloads (12 Months)	717
Downloads (cumulative)	7,331
Average downloads per article	252.79
Average citations per article	6.75

지금 : Military and Intelligence in Digital Forensics

- Military and Intelligence are becoming (have been) much more interested in digital forensics
- With more funding going towards discovering intrusions (security / forensics techniques) knowledge of vulnerabilities is a strategic advantage for a country
- Intelligence gained from digital forensics can be used for offensive and defensive purposes

지금 : The State of Digital Forensic Research

- Currently lead by U.S. and Europe
- Constantly working to collect data or information from any type of device
- Constantly working reliably reduce the amount of data that a human has to look at

지금 : Digital Forensic Science

- Digital Forensic Science is not yet considered a "forensic science"
  - Still a lack of standardization
  - Somewhat a certification problem
  - Common body of knowledge
  - Science vs. Technique
  - Testing
- Digital evidence normally accepted in court (Daubert)

지금 : Digital Forensic Practice

- Drastically different levels of proficiency between countries (and within countries)
- Many countries still have no:
  - Legislation
  - Standards
  - Basic understanding
  - Capacity
  - Equipment
- Countries are really bad at working together

지금 : Bonus – The Public

- More people are getting powerful devices
- Most people have no idea how they work
- Most people have no idea how to secure themselves
- Most people don't understand why they need to secure themselves
- Security vendors and experts make things too hard

Where are we going?

Future: Digital Forensic Research

- Digital forensic research is going beyond information retrieval into automated knowledge acquisition
  - Current stage: http://badsite.com/illegal.jpg
  - Next stage: illegal picture x was traded with suspect IP address 10.0.0.12 at 13:00
- What is needed?
  - Powerful artificial intelligence
  - Automated investigative reasoning
  - Automated legal reasoning (huge knowledge domains)

Future: Digital Forensic Research

- Better understanding of cybercrime and digital forensic investigations to drive police management and tactical strategies
- What is needed?
  - Massive database of past cases (KICS)
  - Data mining to discover patterns and trends
  - High-level officials willing to admit that they may wrong
  - Humans willing to accept evidence over gut instinct

Future: Digital Forensic Research

- Agreed baseline for digital forensics education
- What is needed:
  - A group of countries driving standards together
  - Other countries adopting established best practices
  - Political motivation

Future: Digital Forensic Research

- Data recovery, OS analysis, memory analysis, tool testing, standards and data reduction will continue (forever?)

Future: Digital Forensic Research

- IoT is the next big challenge, mostly because no one really knows how it's different yet
  - Incorporates embedded devices, cloud, human interface devices, traditional computers, and who knows what else

(Far) Future: Digital Forensic Research

- Self-driving cars will spawn an advancement in a number of technologies, including AI
  - Exploitation could kill
  - Advanced tech needed may be used for criminal purposes

(Far) Future: Digital Forensic Research

- Digital implants are coming
  - Bio-sensors – already used in court! (fitbit)
  - Storage
  - Data and person will be afforded same rights

What is really needed?

What is *needed*?

- Currently the gap in knowledge and capacity of different countries is so large that working together is not practical
- Improved international cooperation based on justice, not nationality (a common goal)
- Improved, transparent research practices
  - There is currently too much duplication (and we are a small field)
  - Public research helps understanding and policy alignment
- Basic, easy to use tools and methods shared globally
- Cheap / free tools that are effective in dealing with multiple languages
- Global infrastructure directly embedded in local cyber investigation units

Cybersecurity in South Korea

Lets make the world a safer place!

Thank you!

Joshua@cybercrimetech.com