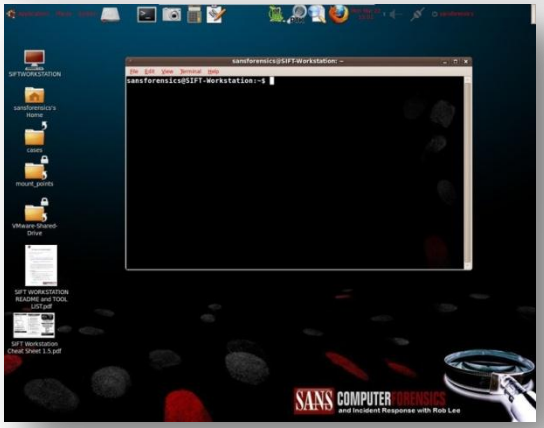
Time and Place: Hunting Evil with Atemporal Time Line Analysis

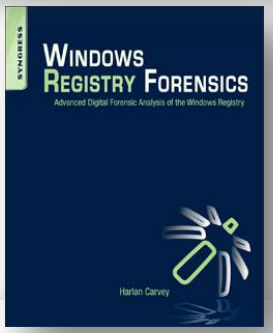
Doing it Weird

Ob bio



SANS COMPUTER FORENSICS and Incident Response with Rob Lee

metasploit®



dave hull

@davehull I'm here.

Recently realized I know nothing. I don't do dongles.

http://trustedsignal.com

time lines

brief intro by way of a case study…

- case background:
  - Discovered in Q1 2011
  - irc bot <- yeah, old skool

find it

Photo source - http://www.flickr.com/photos/theplanetdotcom

reality

Photo source - http://www.flickr.com/photos/zeevveez/

investigative plan

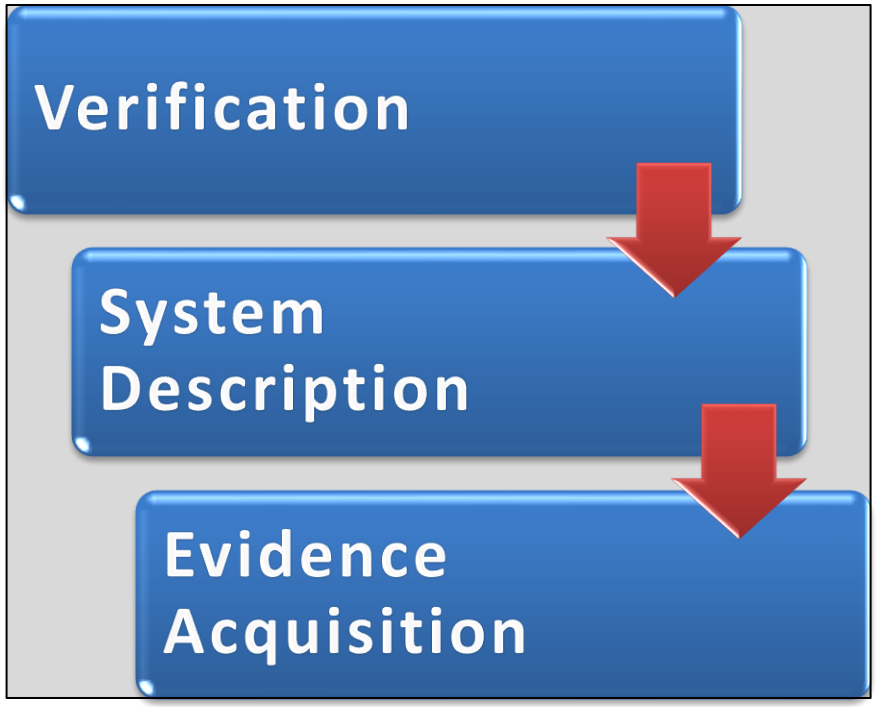
where’s the attacker’s code?

how’d they get in?

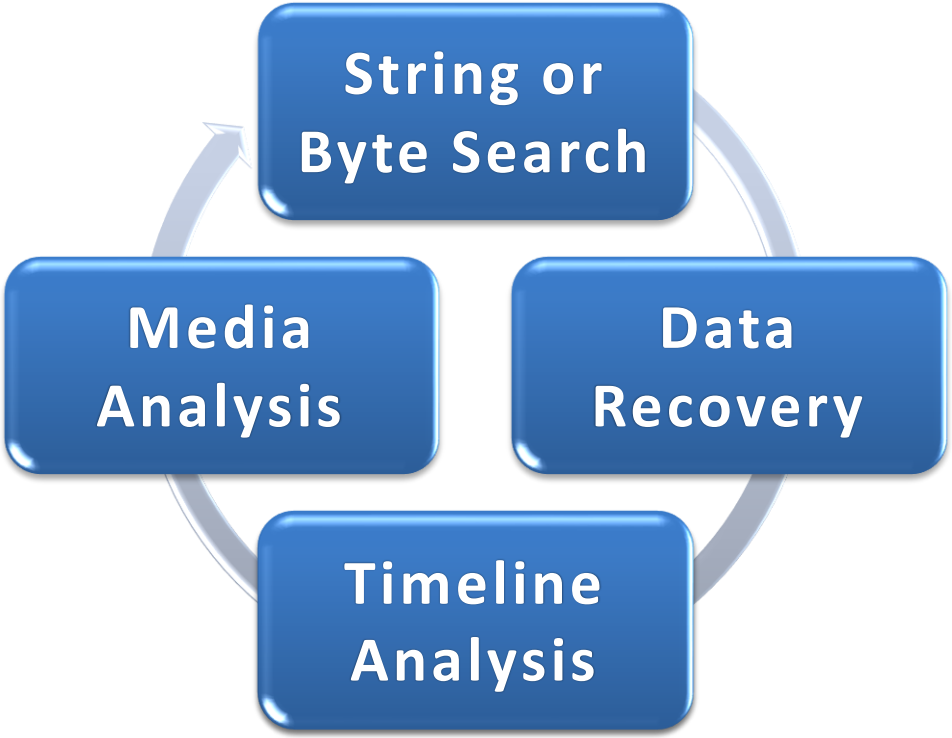
what did they do/take?

investigative methodology

Incident Response And Evidence Acquisition



Investigation and Analysis



Source – SANS Forensics 508: Advanced Computer Forensic Analysis and Incident Response

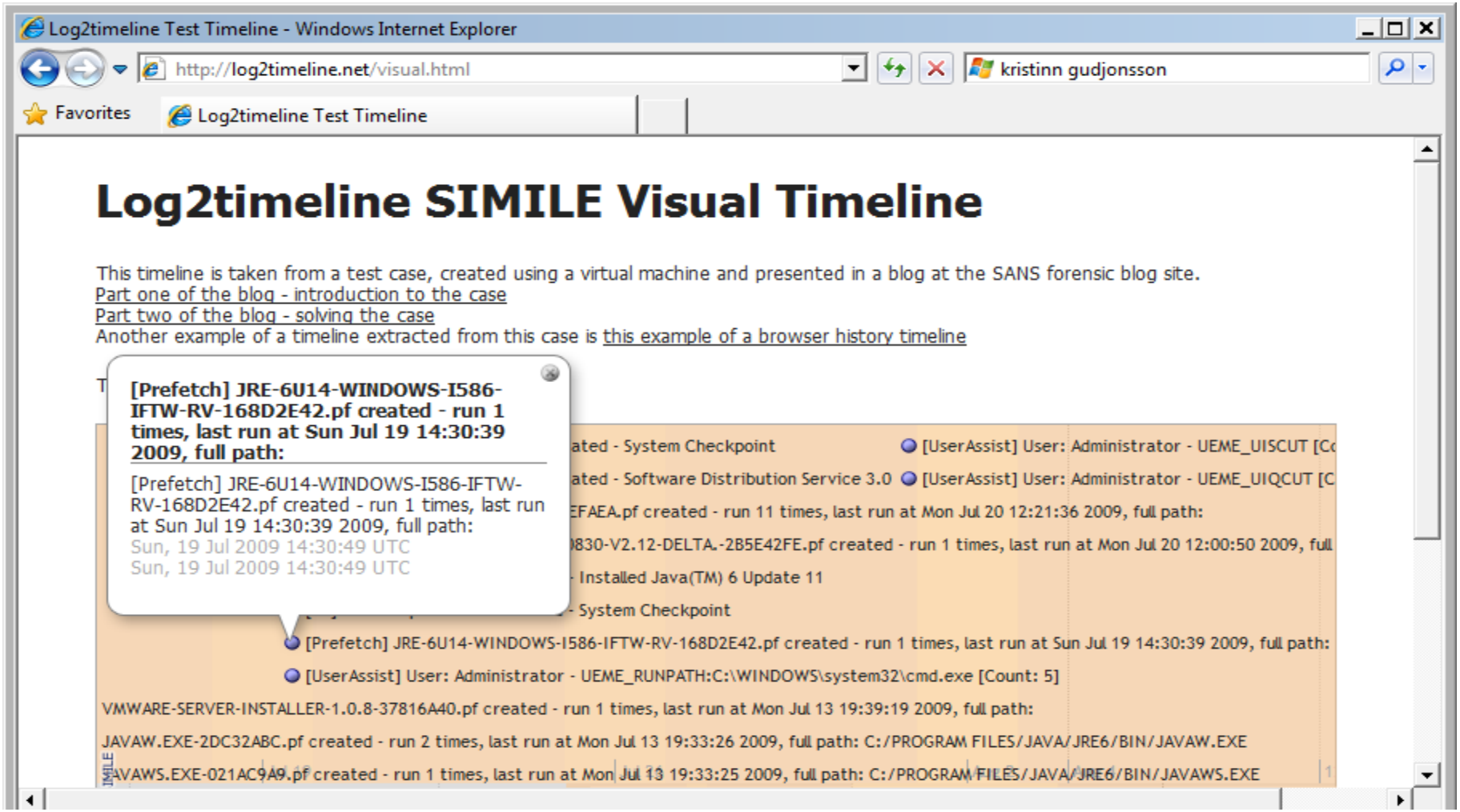
Reporting Results

traditional time lines

taunting the demo gods

Photo source - internets

new school time lines



Source – http://log2timeline.net

a·tem·po·ral

“considered without relation to time”

file systems: how do they work?

Photo source - http://www.flickr.com/photos/alexwatkins123

metadata

Photo source - http://www.flickr.com/photos/deborahfitchett

metadata demo

towards automation

https://github.com/davehull/body-outliers

standing on Carrier's toes

Automated Digital Evidence Target Definition Using Outlier Analysis and Existing Evidence

Brian D. Carrier
carrier@cerias.purdue.edu

Eugene H. Spafford
spaf@cerias.purdue.edu

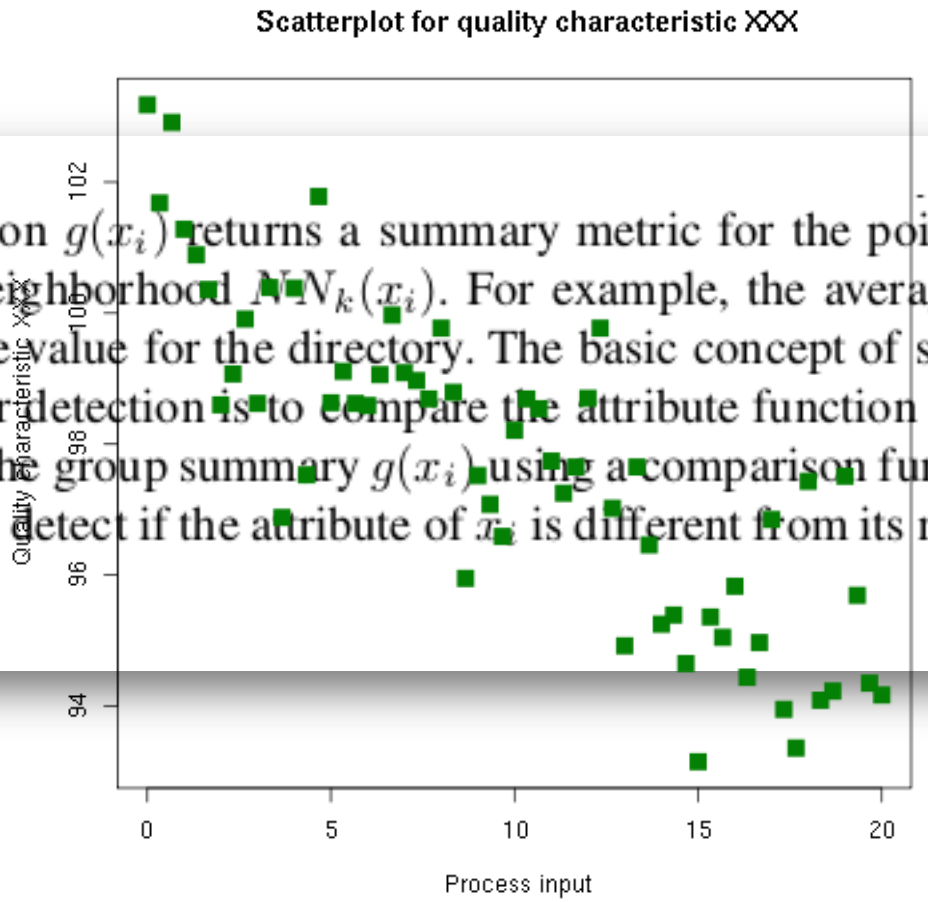
Center for Education and Research in
Information Assurance and Security - CERIAS
Purdue University
West Lafayette, IN 47907 USA

Abstract

Searching for digital evidence is a time consuming and error-prone process. In this paper, we introduce techniques to automate the searching process by suggesting what searches could be helpful. We also use data mining techniques to find files and directories creations more thorough and accurate because the tool keeps track of what searches still need to be conducted. We implemented four analysis tools and one suggested additional searches based on existing evidence and the other three used different outlier analysis algorithms. The implementations were run on the file system data from a compromised Linux system.

Souce - http://www.dfrws.org/2005/proceedings/carrier_targetdefn.pdf

meta attributes as spatial pts



function $g(x_i)$ returns a summary metric for the points in the neighborhood $NN_k(x_i)$. For example, the average attribute value for the directory. The basic concept of spatial outlier detection is to compare the attribute function $f(x_i)$ with the group summary $g(x_i)$ using a comparison function $h()$ to detect if the attribute of x_i is different from its neighbors.

http://en.wikipedia.org/wiki/File:Scatter_diagram_for_quality_characteristic_XXX.svg

false positives are high

When we look at the combined results we see that the last changed time (C-time) has a high success rate, but less than 10% of the files identified using other attributes were actually related to the incident. Using a θ value of 2 or 3 has little impact because some accuracy rates increase and others decrease.

Souce - http://www.dfrws.org/2005/proceedings/carrier_targetdefn.pdf

future dev

- Find outliers for meta element within the set of another meta element, i.e.
  - for files created on a given day, what is the average metadata address, what are the outliers?
  - for files in a given metadata address range, what are the date outliers?

future dev

- combine with external data sources, i.e.
  - are outliers packed?
  - correlate with autoruns
- graphing, i.e.
  - scatterplot metadata as spatial points per Carrier
- …

questions?

contact:

trustedsignal.com

twitter.com/trustedsignal

Thank you