WHAT FORENSIC TECHNIQUE(S) DO YOU FEEL EVERY INVESTIGATOR SHOULD KNOW BUT CURRENTLY DOESN'T?

2010 EU Digital Forensics and Incident Response Summit
Who am I?

• M.Sc. in computer and communication network engineering
• Team leader – information security at Skyggnir
• Worked in forensics and information security since 2005
• SANS certifications: GCIA, GCIH, GCFA gold
• SANS mentor
• Author of log2timeline
• Blog author at the SANS forensics blog
• Author of the blog: blog.kiddaland.net
First a Short Disclaimer

- I haven’t used any of the big named brands
- I need to work on a very limited budget
  - The “xxd/vim/grep/awk is just as good as Forensicator Pro, just think harder” kind of budget
- So my answer is biased with my experience of doing forensics on a shoe string budget
  - There are no dongles on my desk
Get to Know a Scripting Language

- For me this is a very important tool
  - Perhaps the most used one
- Does not really matter which one
  - Perl, python, ruby, ....
- Use the one you are most comfortable with
  - Each one has its strengths and weaknesses
  - And if you know one, it’s easy to learn the others as well
Why Do I Believe This is Important?

• Understanding of a programming language makes it easier to understand how programs work
  – Thus understand how they behave
  – Makes understanding artifacts easier
• Why a scripting language?
  – Easy to write a quick script
  – Usually include several libraries to make life easier
  – No need to constantly compile code before testing
• Sometimes you simply come across something that no tool is capable of doing
  – And sometimes it can be done easily with a short script
• Easy to write script to automate some tasks that are done repeatedly
  – Can shorten the investigation time by automating repetitive tasks
Other Techniques

• Consider using the built-in *NIX tools to make things easier
  – sed, awk, grep to name a few

• Take a time to get to know them
  – Write a quick bash script to utilize them to perform some repetitive tasks
  – Can save the investigator considerable time

• Learn about networking
  – Know how TCP/IP works, and how to read packets
  – Makes communications between applications easier to understand
  – If you can get a copy of a network capture it can often make life easier
  – Network capture can be a gold mine, although not always available
Questions?

Kristinn Guðjónsson
kristinn@log2timeline.net
kristinng@skyggnir.is

Skyggnir
Borgartún 37
105 Reykjavík
Iceland
Telephone: 516 1000
www.skyggnir.is