Information Security:
It's Everyone's
Responsibility.

MITS

Cybersecurity

Know Your Network

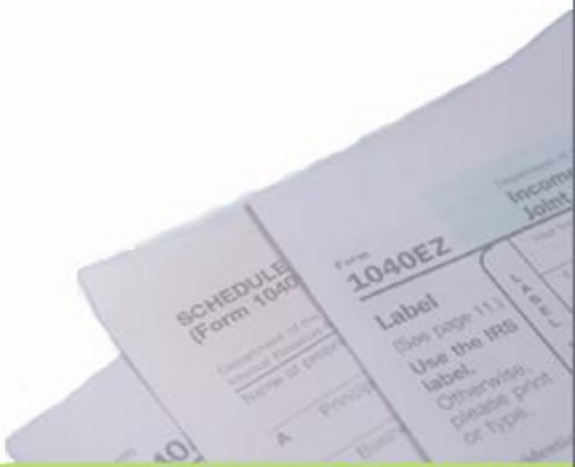
Computer Security Incident Response Center

"Tracking Compliance…Identifying and Mitigating Threats"

Teaming for Results

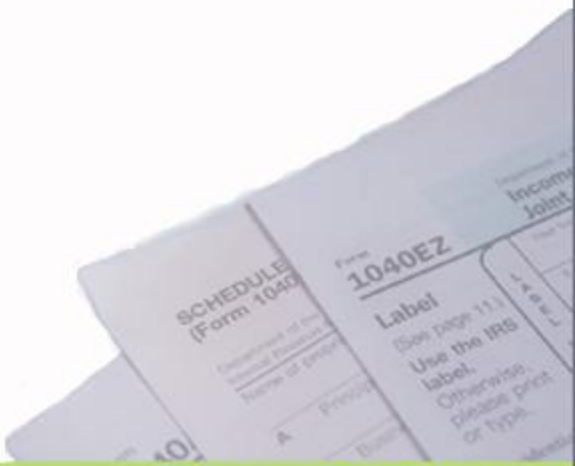
Agenda

- Background
- What does "Know Your Network" mean?
- About me
- Breadth, then depth
- Jumping off points approach
- Tiers of joy
- Tier 1 analysis
- Tier 2 analysis
- Tier 3 analysis
- Some interesting examples
- Case study
- Q&A



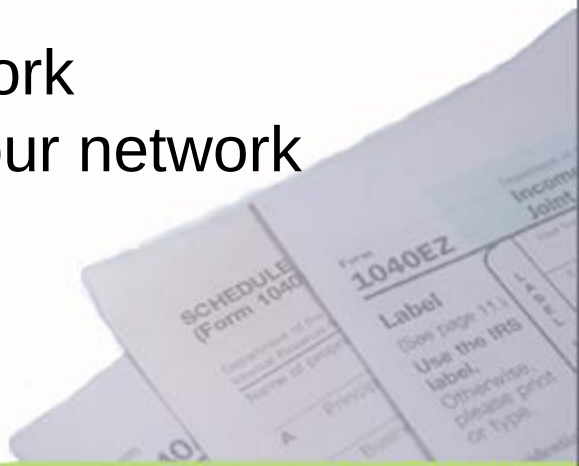
Background

- Networks are large, busy, and complicated (a challenge)
- Data is voluminous (another challenge)
- Need to know what belongs on a network to know what doesn't
- Profiling/modeling an enterprise network is not feasible
- Need to approach the problem in a different way
- Consider a sampling/best approximation approach



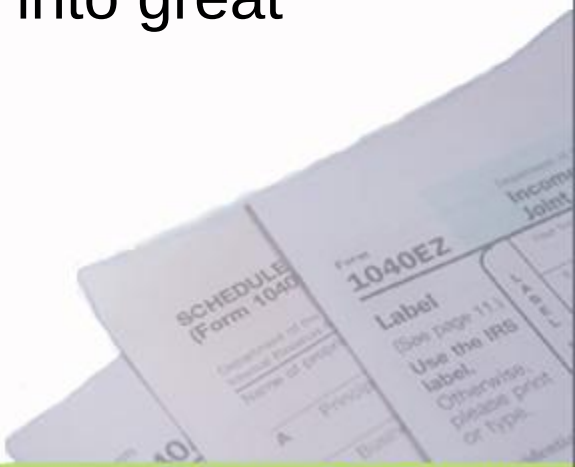
What Does "Know Your Network" Mean?

- Need to know what belongs on a network to know what doesn't
- In practicality, this isn't possible
- Using an organized, well-structured approach to analysis, you can come close
- Close is usually good enough for starters (you're likely to find things you're not finding now)
- Continuously tune and re-evaluate analytical approach as time progresses
- Along the way, you'll be learning your network
- Eventually, you'll come close to knowing your network



About Me

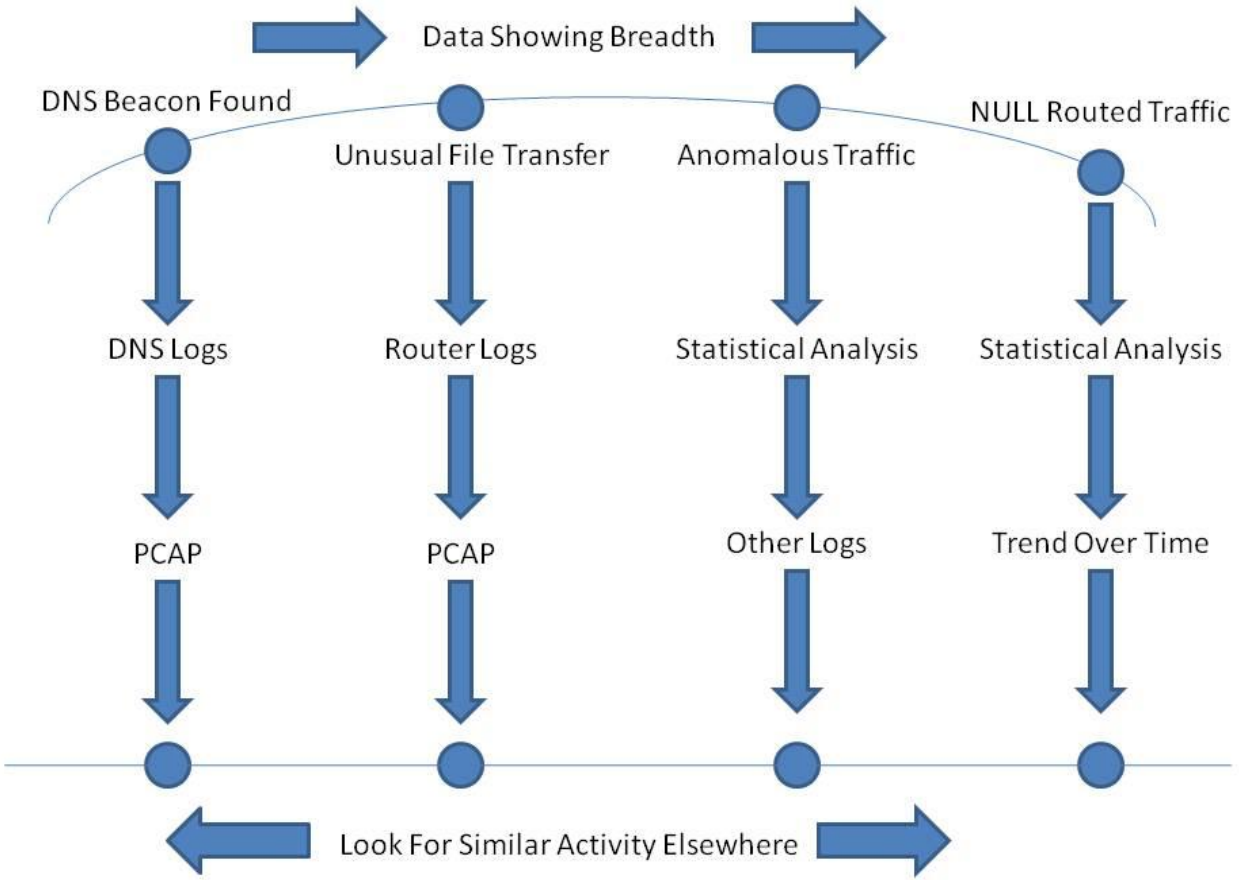
- I don't really like talking about myself
- Briefly:
  - Former Chief of Analysis for US-CERT
  - Currently a consultant focused on helping organizations build and enhance their network traffic analysis programs
  - Also a USAF Reservist focused on network traffic analysis and training analysts
  - Started out as programmer, then transitioned into infosec
  - Lots of experience turning smart people into great analysts



Breadth, Then Depth

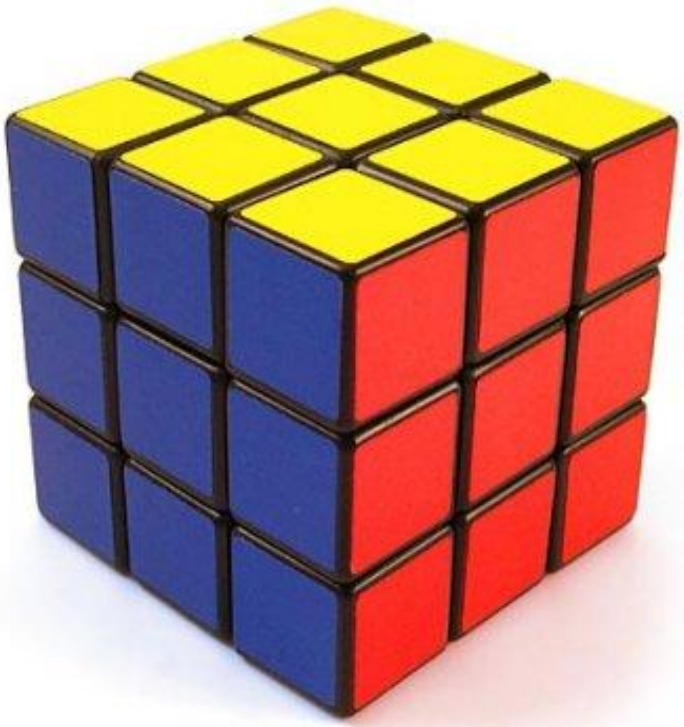
- Seek first to understand, then to be understood

Breadth, Then Depth (Continued)



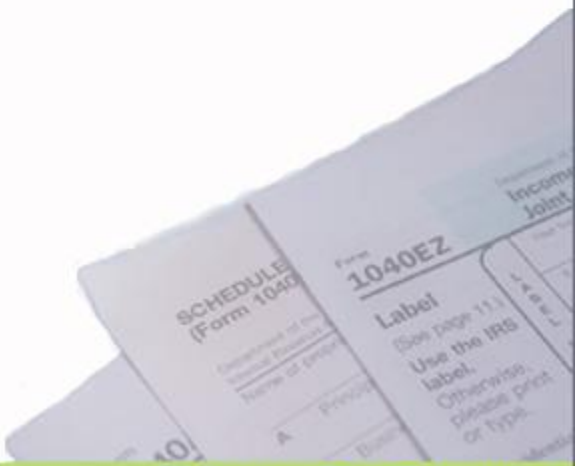
Jumping Off Points Approach

- A large network is essentially a very complicated black box
- Observing the network from many different jumping off points enables us to better understand what may actually be going on inside and facilitates analyst workflow



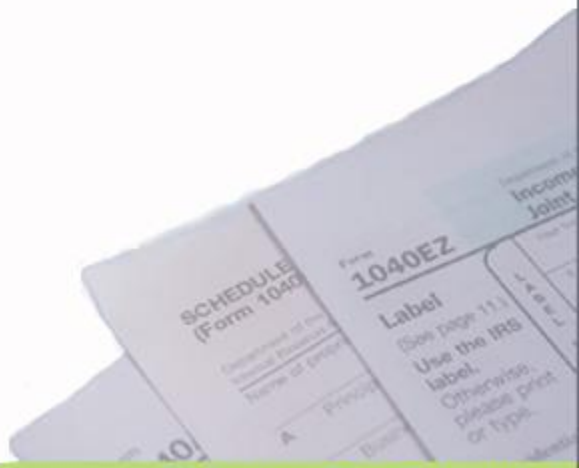
Tiers of Joy

- Tier 1 -- basic analysis used for situational awareness
- Tier 2 -- mid-level analysis used for ad hoc queries and moderately complex queries
- Tier 3 -- advanced analysis (looking for the needle in a pile of needles)



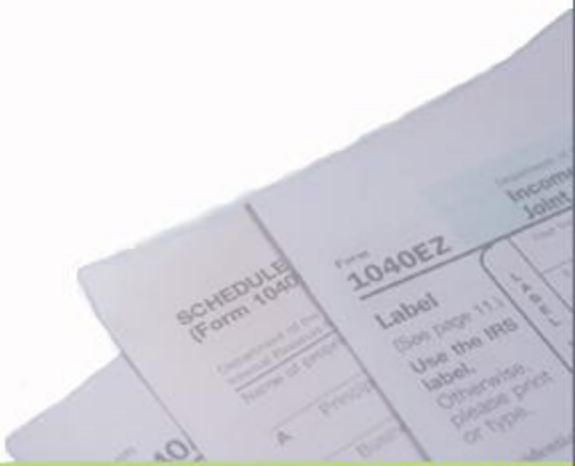
Tier 1 Analytical Methods

- IP watch lists
- Queries keyed on IP address
- Traffic volume
- Sensor up/down status
- Counts
- etc...



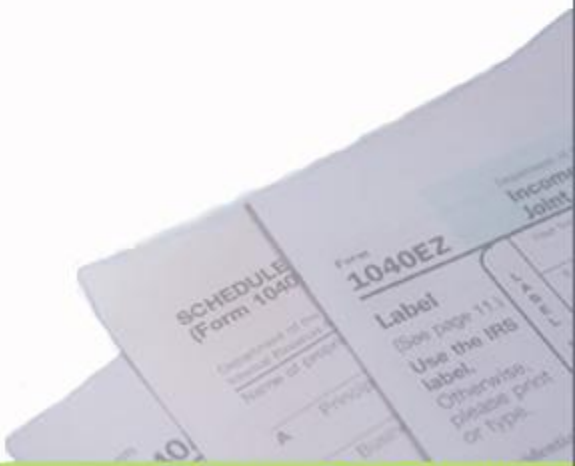
Tier 2 Analytical Methods

- Queries keyed on fields other than IP address
- Queries keyed on more than one field
- Queries looking for anomalies that are moderately difficult to spot
- Correlation with other data sources
- Automation/scripting
- etc...



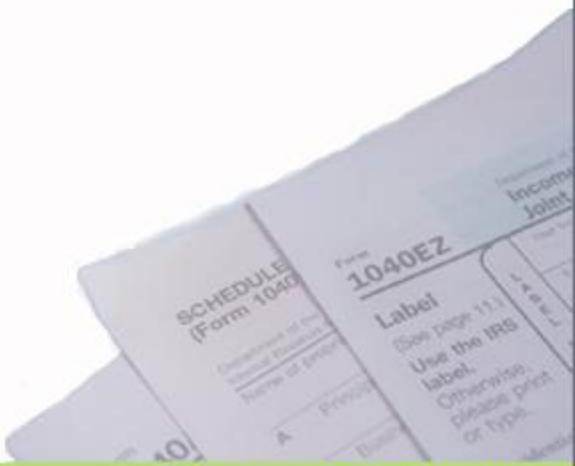
Tier 3 Analytical Methods

- Performing statistical analysis
- Examining how the data inter-relate
- Trending over time
- Trending over other fields
- Reviewing data in 3-tuples not involving time
- etc...



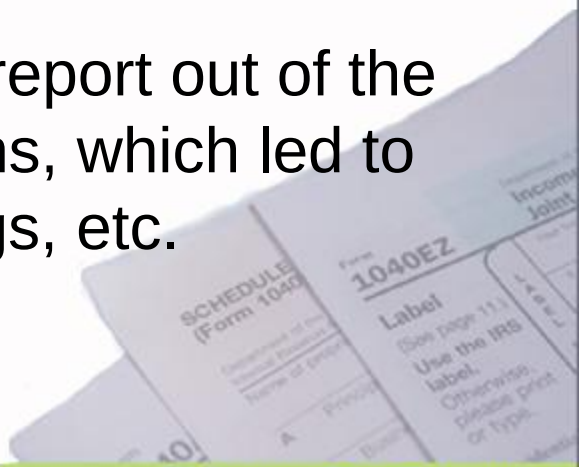
A Few Interesting Examples

- Source port, destination port, number of bytes 3-tuple
- Same number of bytes/packets/flows every N minutes
- Encrypted traffic over unencrypted protocols
- Unencrypted traffic over encrypted protocols
- Large transfers outbound from desktops (not servers -- know your network!)
- Packets not conforming to IETF standards
- And many more!



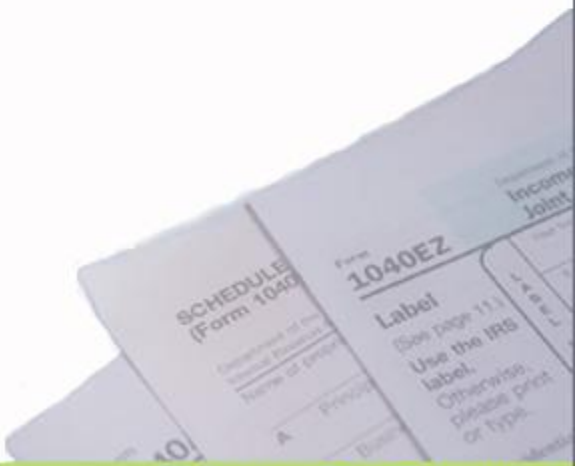
Case Study

- Studied a large, enterprise network over a week's worth of data using the approach described here
- Interesting findings included (but weren't limited to):
  - The network routed far more protocols than most people realized it did
  - Like it or not, the network was already routing IPv6
  - Some of the traffic found was designed to fly under the radar and would not be caught by even the most current signatures (Donald Rumsfeld)
  - Continuous tuning is necessary -- the report out of the findings generated interest and questions, which led to more analysis, which led to more findings, etc.



Acknowledgments

Thank you IRS CSIRC!



Q&A

Question/Comments/Produce?

Josh Goldfarb
President
NetflowData LLC
(240) 393-1314 (m)
(240) 235-3744 (f)
josh@netflowdata.com
http://www.netflowdata.com/