DFRWS
DIGITAL FORENSIC RESEARCH CONFERENCE

These Logs Were Made for Talking

By

Matt Bromiley

Presented At

The Digital Forensic Research Conference

DFRWS 2014 USA Denver, CO (Aug 3rd - 6th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org

These Logs Were Made for Talking

Matt Bromiley – @505Forensics

Agenda

- $ whoami
- $ cat why_are_there_so_many_textfiles
- $ elasticsearch & logstash & kibana
- $ ./elk_stack setup
- $ demo

These Logs Were Made for Talking

whoami

whoami

- Matt Bromiley
- Based in Dallas, TX; formerly Annapolis, MD

- Senior Cybercrime and Incident Response Consultant
- Cybersecurity Graduate Student (In-Progress)

- http://www.505forensics.com
- @505Forensics

whoami (obligatory disclaimer)

I’m just going to put this here:

My opinions are my own; not my employers.

Also, this isn’t a product endorsement. Some things just work better than others.

These Logs Were Made for Talking

cat why_are_there_so_many_textfiles

why_are_there_so_many_text_files

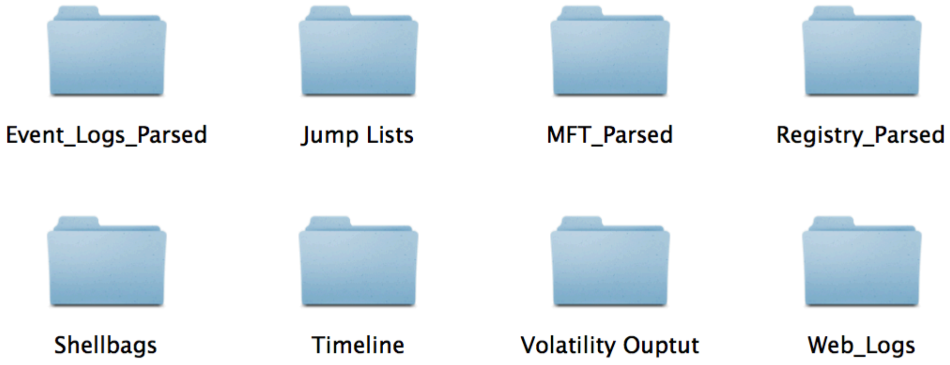
- Face it: We love flat text

- Artifacts look better in flat text:
  - Registry
  - $MFT
  - Event Logs
  - Web Logs
  - ${insert_your_favorite_log_here}
  - Log2timeline/Plaso (all of the above)

why_are_there_so_many_text_files (cont.)

- Flat text allows us to maintain our command line kung fu
  - awk | sed | grep | sort | split | tr | join
  - Writing custom scripts to handle data

- Now we have more flat text output; just smaller and refined



why_are_there_so_many_text_files (cont.)

Text File Issues

- Structure is hard to transfer
  - Tough to join someone else in The Matrix

- Little to no enrichment; text is still just text
  - Keep your browser handy
  - Air-gapped lab?

- Every try to show off 10 text files to management?
  - Nope, nope, nope

- I just want to analyze

These Logs Were Made for Talking

elasticsearch & logstash & kibana

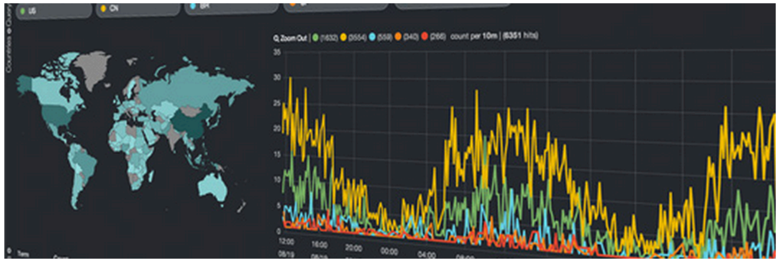
The ELK Stack

The ELK Stack

elasticsearch.

Elasticsearch– Distributed, restful index engine based on Apache Lucene with free text search

Logstash – Manage all those text files; bring any ingestible data into a central repository for analytics



Kibana – Visualize your data inside Elasticsearch with interactive pages, custom visualization options

More info at http://www.elasticsearch.org - more than I could ever talk about

The ELK Stack (cont.)

The process flow:

Logstash -> Elasticsearch <- Kibana

- Elasticsearch: Schema-less, JSON storage
- Kibana: Angular webapp to interact with Elasticsearch

- **Logstash: The log shipper; power lies in the config files**

The ELK Stack (cont.)

Logstash config format:

`input {} – Where is it?`

`filter {} – What am I doing with it?`

This is where we enrich!!

`output {} – Where do you want it?`

The ELK Stack (cont.)

Logstash config files allow us to :

- Handle a large variety of data types
- Enrich data our data with geo-location, DNS lookups, etc.
- Mutate, transform, combine data in-motion; no more “prepping” before ingestion
- Input “non-text” data, such as netflow, Twitter, SQLlite, syslog

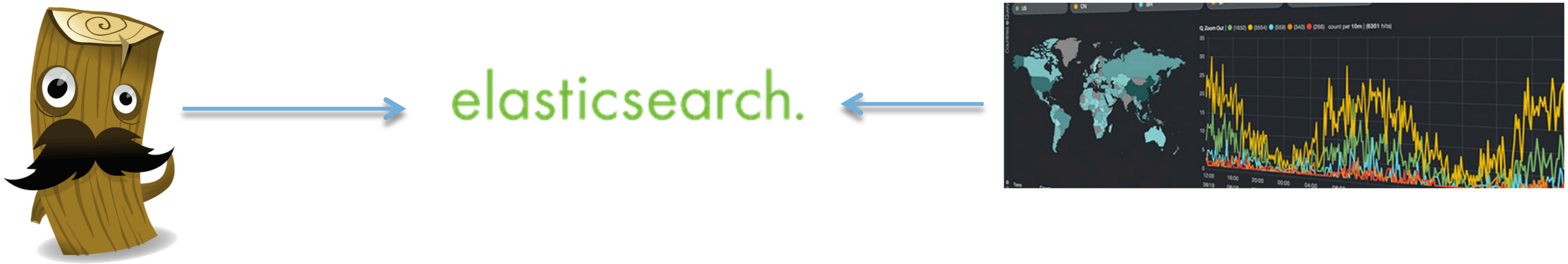
These Logs Were Made for Talking

./elk_stack_setup

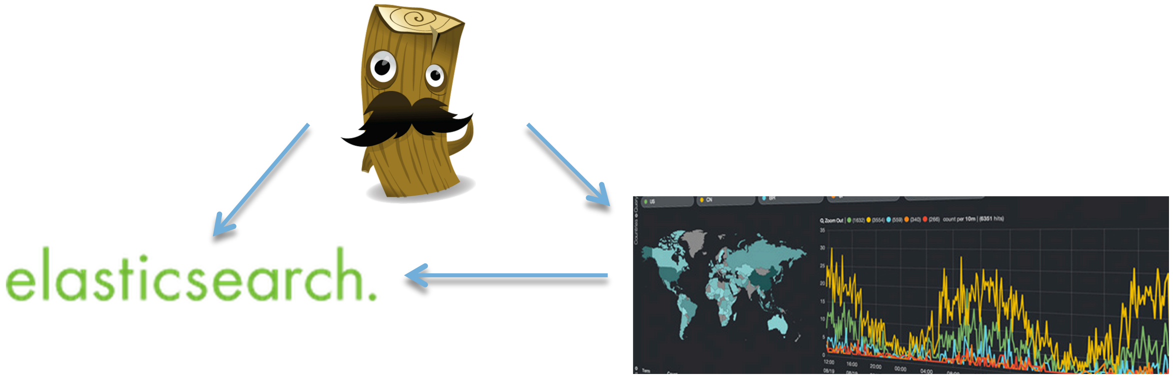
./elk_stack_setup

Two setups:

- **Mature lab**



- **On-fly-analysis, rapid triage**



These Logs Were Made for Talking

Demo

(finally)

Questions?

Matt Bromiley

@505Forensics

505forensics@gmail.com

http://www.505forensics.com

Thank you!

Extra thanks to:
DFRWS

Elasticsearch Crew

All the forensicators out there