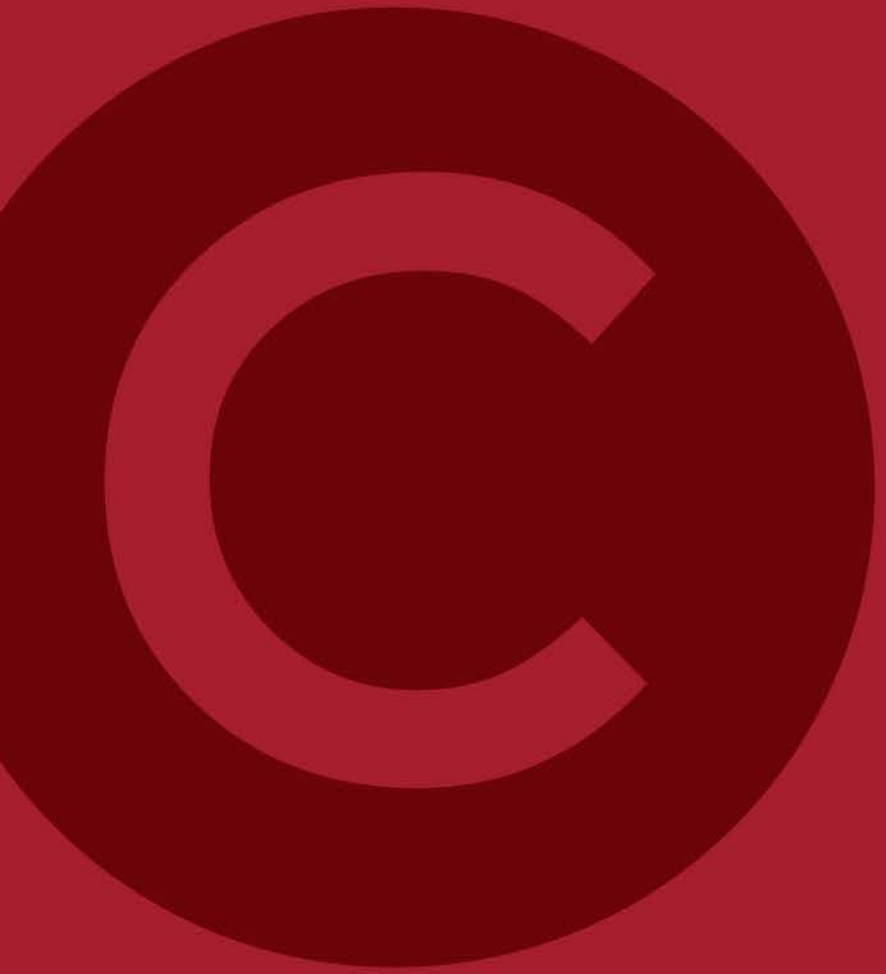
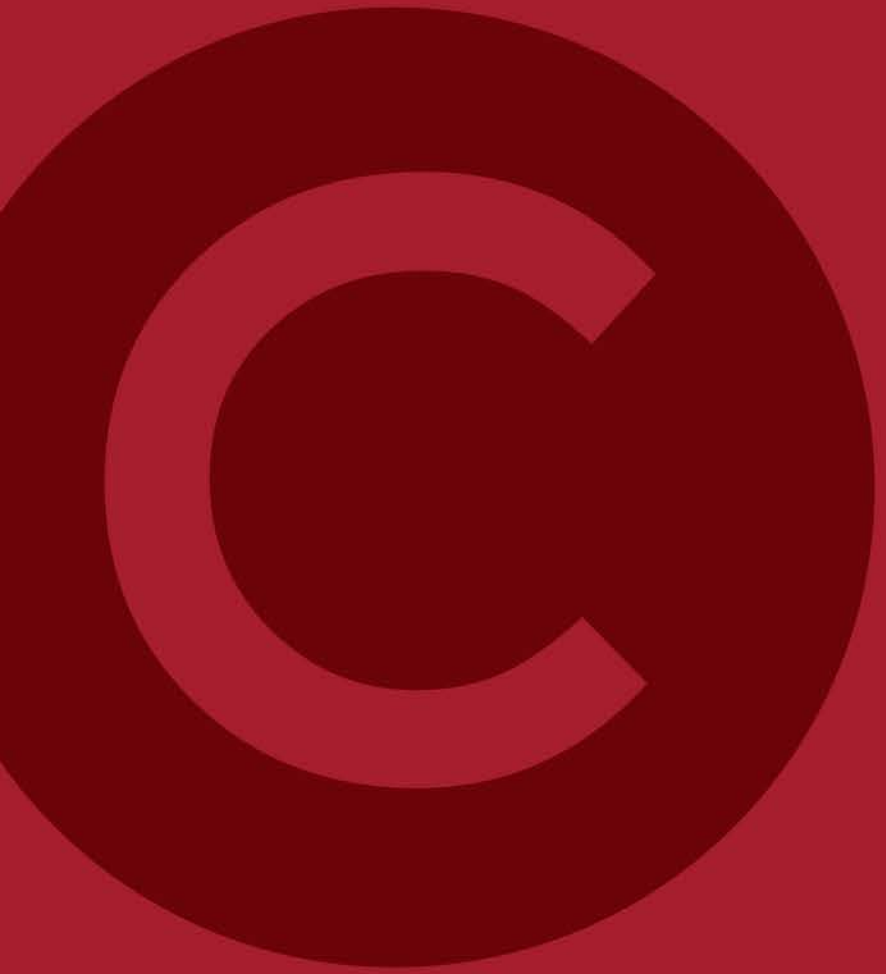

CRYPSIS™
It’s about time...
The only timeline tool you’ll ever need!



Introduction

about me...

- Jon Tomczak
  - → Senior Consultant – Crypsis
  - → Game Dev turned Forensicator
  - → Past:
    - Started TZWorks in 2006
    - Consultant at Mandiant



IR Data Analysis

sources of data (raw)

- Log Data
  - → Web
  - → Firewall
  - → AV
  - → Email
  - → Application
- System Data
  - → Filesystem
  - → Events
  - → Registry/Properties
  - → Application
- Network Data
  - → NetFlow
  - → Packet Capture

sources of data (tools)

- Many different tools on the market to analyze the same artifact
  - → Some work better than others for different tasks

All tools with their own standard for output

Comma separated

What about filenames

Lets put some quotes “”s

Pipe delimited

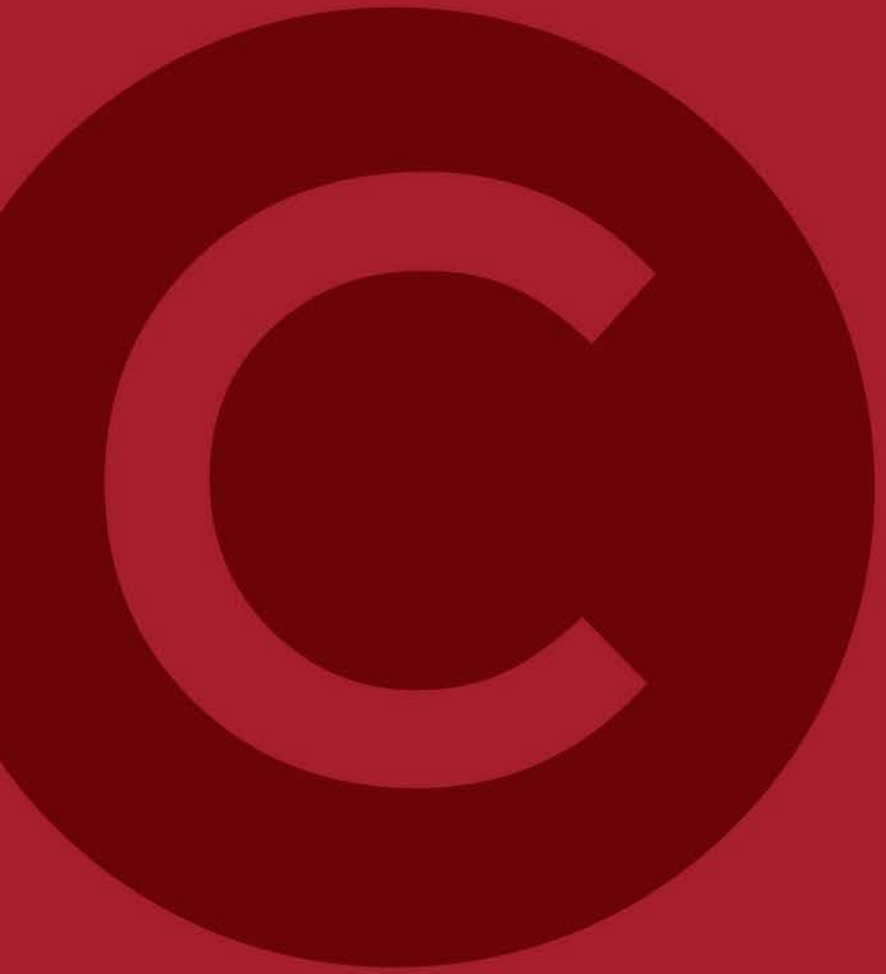
With spacing?

What about Command Arguments?

Do we need to escape the “”s in the command?

What about the nested “”s?

JSON? XML?



Timestamps!?!

sources of data (timestamps)

May 8, 2009 5:57:51 PM
Mon Jan 2 15:04:05 2006
Mon Jan 2 15:04:05 MST 2006
Mon Jan 02 15:04:05 -0700 2006
Monday, 02-Jan-06 15:04:05 MST
Mon, 02 Jan 2006 15:0 4:05 MST
Tue, 11 Jul 2017 16:28:13 +0200 (CEST)
Mon, 02 Jan 2006 15:04:05 -0700
Mon Aug 10 15:44:11 UTC+0100 2015
Fri Jul 03 2015 18:04:07 GMT+0100 (GMT Daylight Time)
07/Mar/2004:17:26:30 -0800
12 Feb 2006, 19:17
2013-Feb-03
3/31/2014
03/31/2014
08/21/71
8/1/71
4/8/2014 22:05
04/08/2014 22:05
04/2/2014 03:00:51
8/8/1965 12:00:00 AM
8/8/1965 01:00:01 PM
8/8/1965 01:00 PM
8/8/1965 1:00 PM
8/8/1965 12:00 AM
4/02/2014 03:00:51
03/19/2012 10:11:59
03/19/2012 10:11:59.3186369
2014/3/31
2014/03/31
2014/4/8 22:05
2014/04/08 22:05
2014/04/2 03:00:51
2014/4/02 03:00:51
2012/03/19 10:11:59
2012/03/19 10:11:59.3186369
2006-01-02T15:04:05+0000
2009-08-12T22:15:09-07:00
2009-08-12T22:15:09
2009-08-12T22:15:09Z
2014-04-26 17:24:37.3186369
2012-08-03 18:31:59.257000000
2014-04-26 17:24:37.123
2013-04-01 22:43:22
2014-12-16 06:20:00 UTC
2014-12-16 06:20:00 GMT
2014-04-26 05:24:37 PM
2014-04-26 13:13:43 +0800
2014-04-26 13:13:44 +09:00
2012-08-03 18:31:59.257000000 +0000 UTC
2015-09-30 18:48:56.35272715 +0000 UTC
2015-02-18 00:12:00 +0000 GMT
2015-02-18 00:12:00 +0000 UTC
2017-07-19 03:21:51+00:00
2014-05-11, 08:20:13,787

sources of data (timestamps)

- Many different variations to represent time
  - → Identified over 100 different timestamp formats

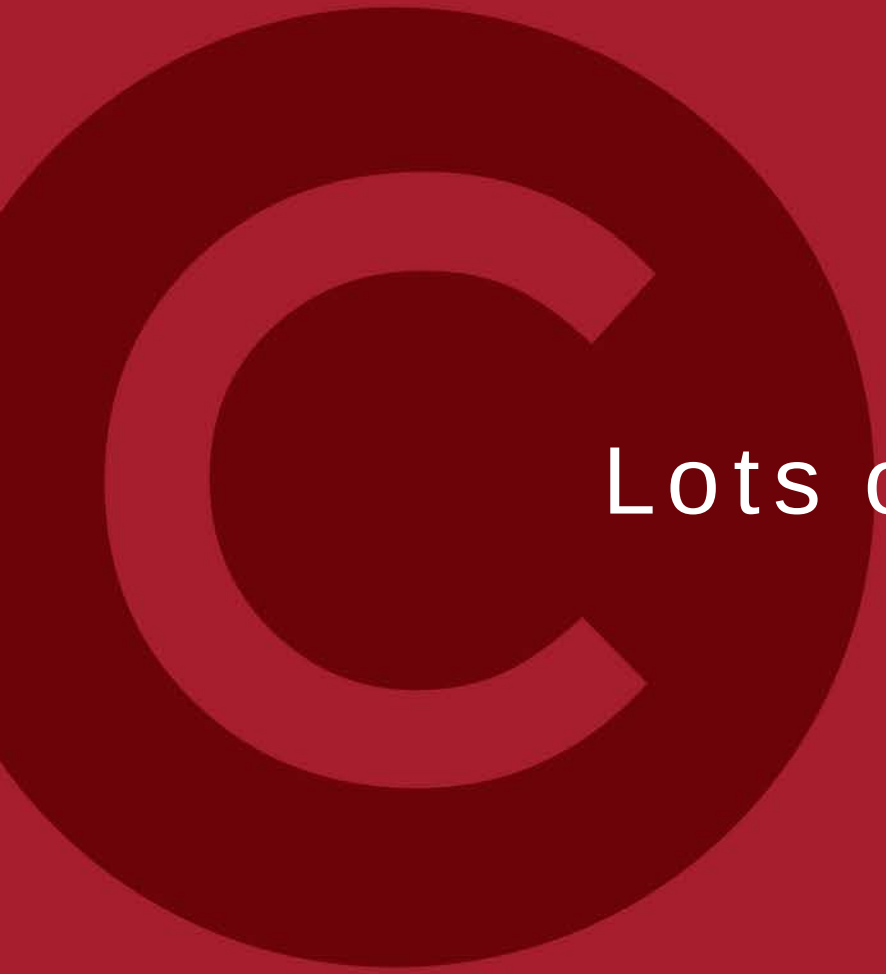
- Will Excel take them all?
  - → Only if formatted correctly, that means no foreign spaces or characters
  - → Sorting for earliest? Uhhh… let's data wrangle that first

professional data wrangler

“Data wrangling is the process of transforming and mapping data from one “raw” form into another format with the intent of making it more appropriate and valuable for a variety of downstream purposes such as analytics”

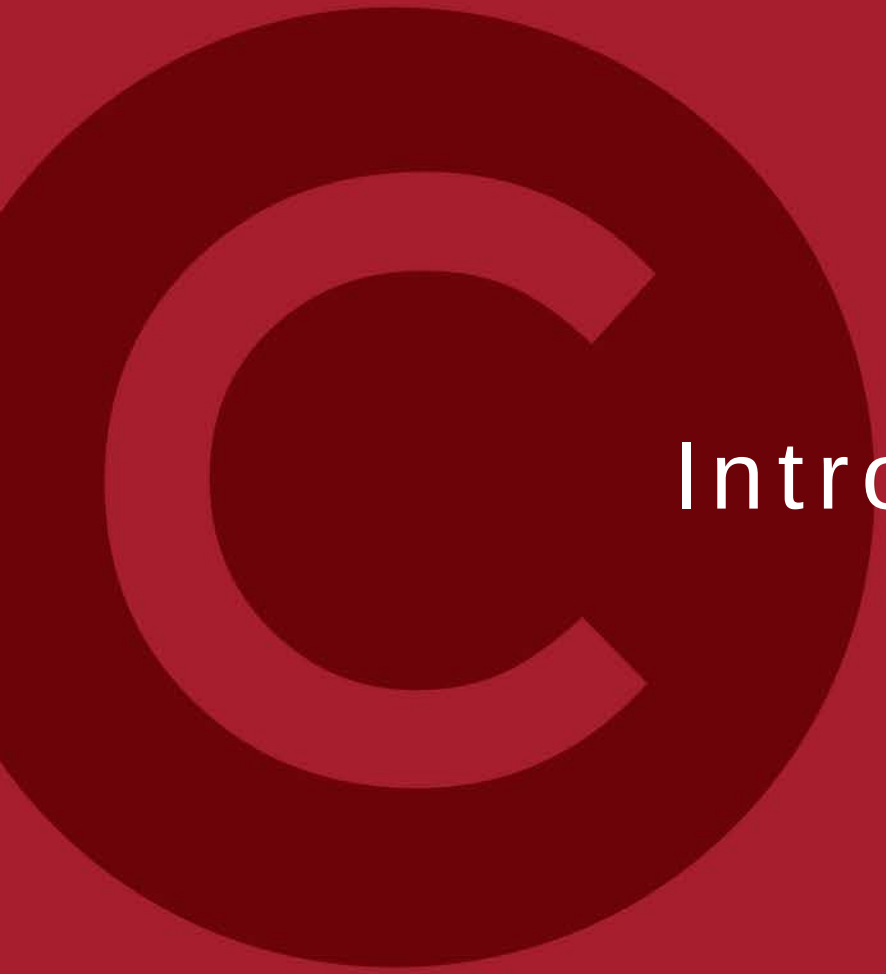
too much data...

- Lots of System Activity?
  - → File Shares
  - → Brute forcing
  - → Ransomware
  - → Activity across multiple endpoints
- Noisy Networks?
- Activity spanning across several months/years?
- SSD's have tons and tons of data in unallocated
  - → Laptop had 55 million USN Journal records in unallocated space
- Volume shadows?
  - → System data multiplier (x2-x7)



Lots of data is good... but

DATA OVERLOAD!



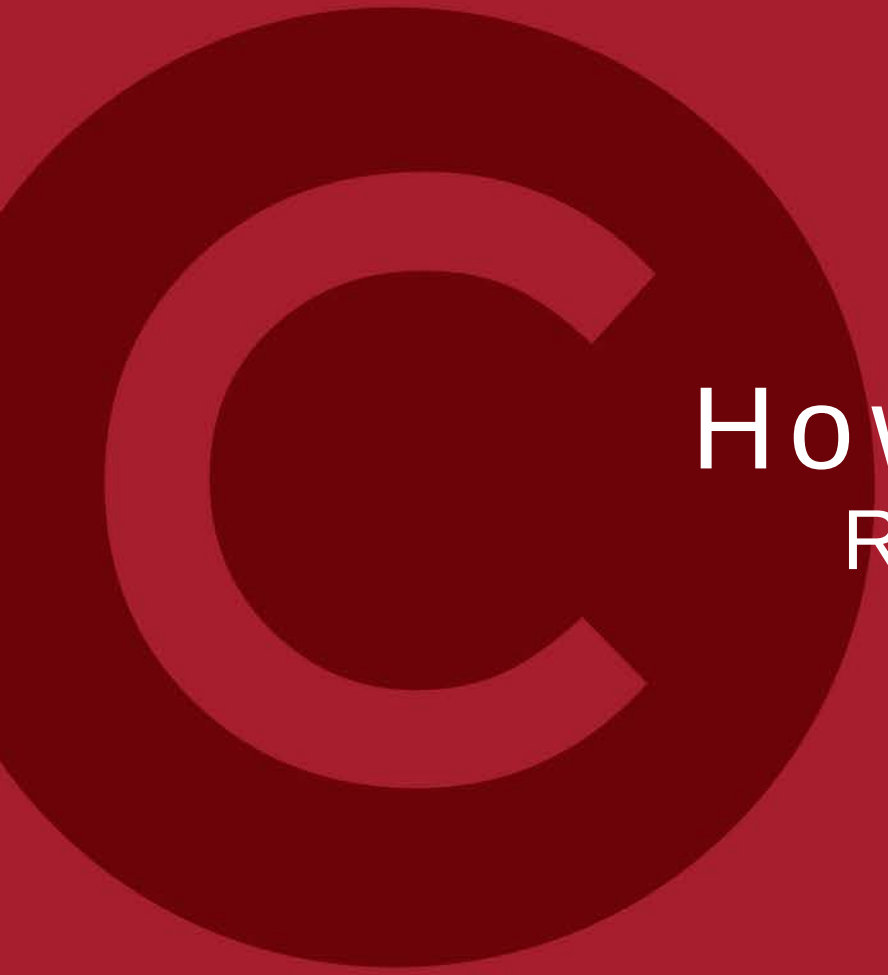
Introducing TimeFrag

what's timefrag?

- Tool to analyze all delimited data, JSON, and XML
- Create timelines with specified data
- Time and metadata filters, using common query expressions
- Tag and comment on specific records
- Reporting

what's timefrag? (continued)

- Written in Golang, C, and the w2ui JavaScript framework
- OS Agnostic
- Static Binary (10 MBs)
- Portable
- Resource Light
- Leverages SQLite databases
- Web interface

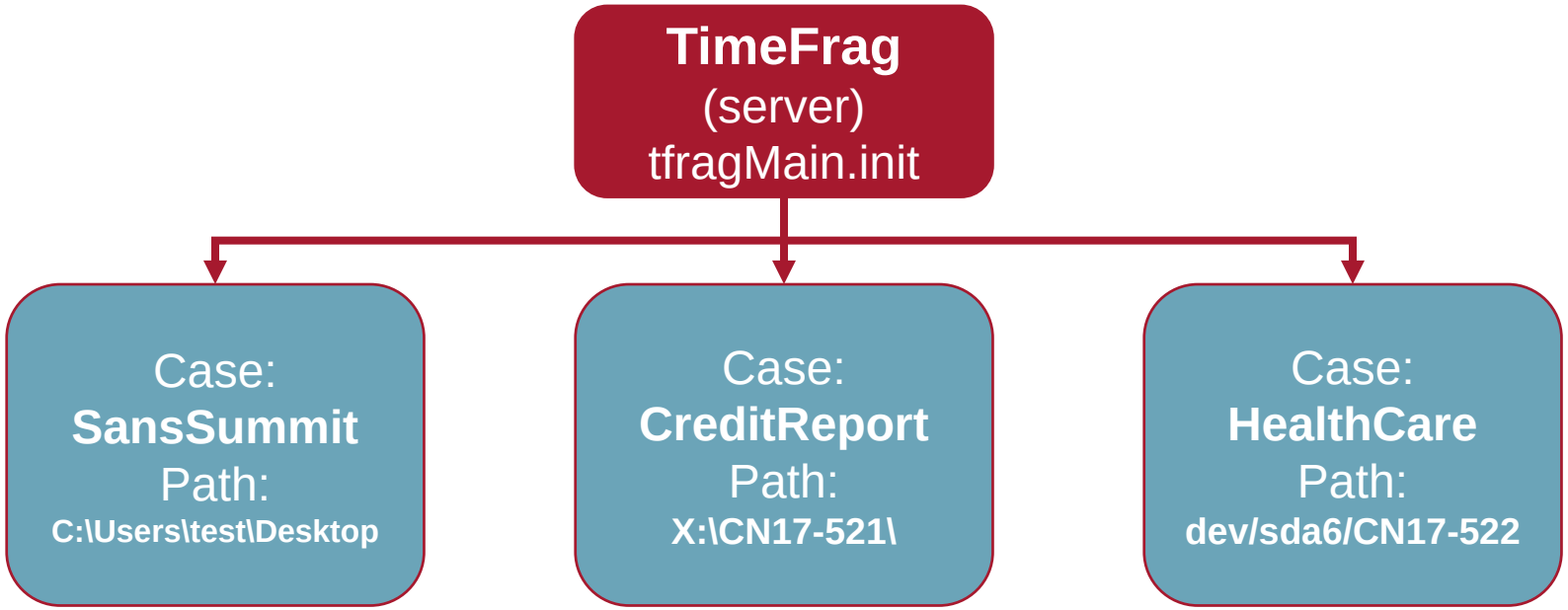


How does it work?

Recorded Demo #1

creating a new case

- Cases can be created on local or external media
- TimeFrag stores all case related data in a user specified directory



adding data: Linking vs Uploading

- Linking accesses local or network resources:
  - → Network File Shares
  - → External USB drives
  - → Local Storage

- Uploading data will copy data from a client to the server
  - → Copied to case directory

viewing data

- Metadata is hashed to identify data types
  - → Delimited data (, | ; ‘ ‘ \t)
  - → JSON tokens
  - → XML tokens (later update)

- Similar Data is viewed in a grid based on hash

querying data

- Data can be queried based on popular syntax
  - AND
  - OR
  - NOT
  - =
  - “”
  - ()
  - *

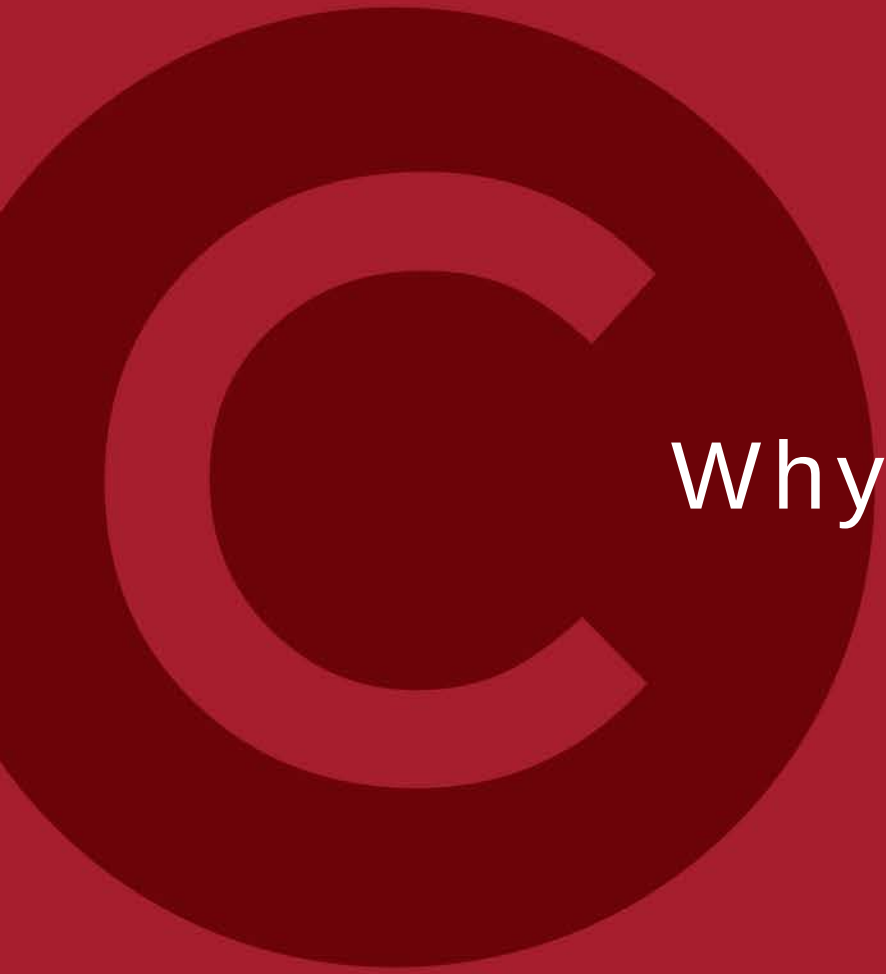
creating timelines

- Timelines can be quickly created or destroyed
  - → A five million record timeline can be generated in 60 seconds or less

- Building a timeline
  - → Select documents
  - → Select metadata
  - → Select date

Creating a Timeline

Recorded Demo #2



Why would I use this?

case study

- Linux Web Server
- Windows Domain Controller
- Seven Windows Laptops
- Twelve MacBooks

data agnostic

- Lots of great tools being built but with no standard output
- Provides a means to accept any data from any source
- Data can be standardized for analysis purposes

data minimization

- Faster analysis
  → Less but targeted data equals finding evil faster
- Analyze multiple systems simultaneously
  → Analyze previously tagged events for context
- Trim unwanted data
  → Reduce the amount of overall data to hunt through

team interaction

- Multiple users can analyze data simultaneously
  - → Multi-threaded application – multiple timelines can be spawned and viewed
- Commenting and tagging
  - → Comments and tags are persistent across the case
- Faster report generation

Questions/Comments?

www.crypsisgroup.com