splunk> .conf2017

Forensic Investigator Splunk App

~~2600~~ ~~2800~~ 2900 Downloads Later

Tony Lee | Sr. Technical Director @Cylance – "Splunk Guy"

Kyle Champlin | Global Strategic Alliance @Splunk – Splunk Ninja

September 2017 | Washington, DC

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

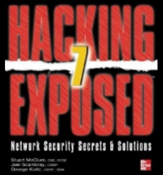
The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

$ whoami

In pictures!

- Tony Lee
  - Sr. Technical Director at Cylance
    - Forensic Investigator Developer

- Kyle Champlin
  - Global Strategic Alliances at Splunk
    - Forensic Investigator Developer



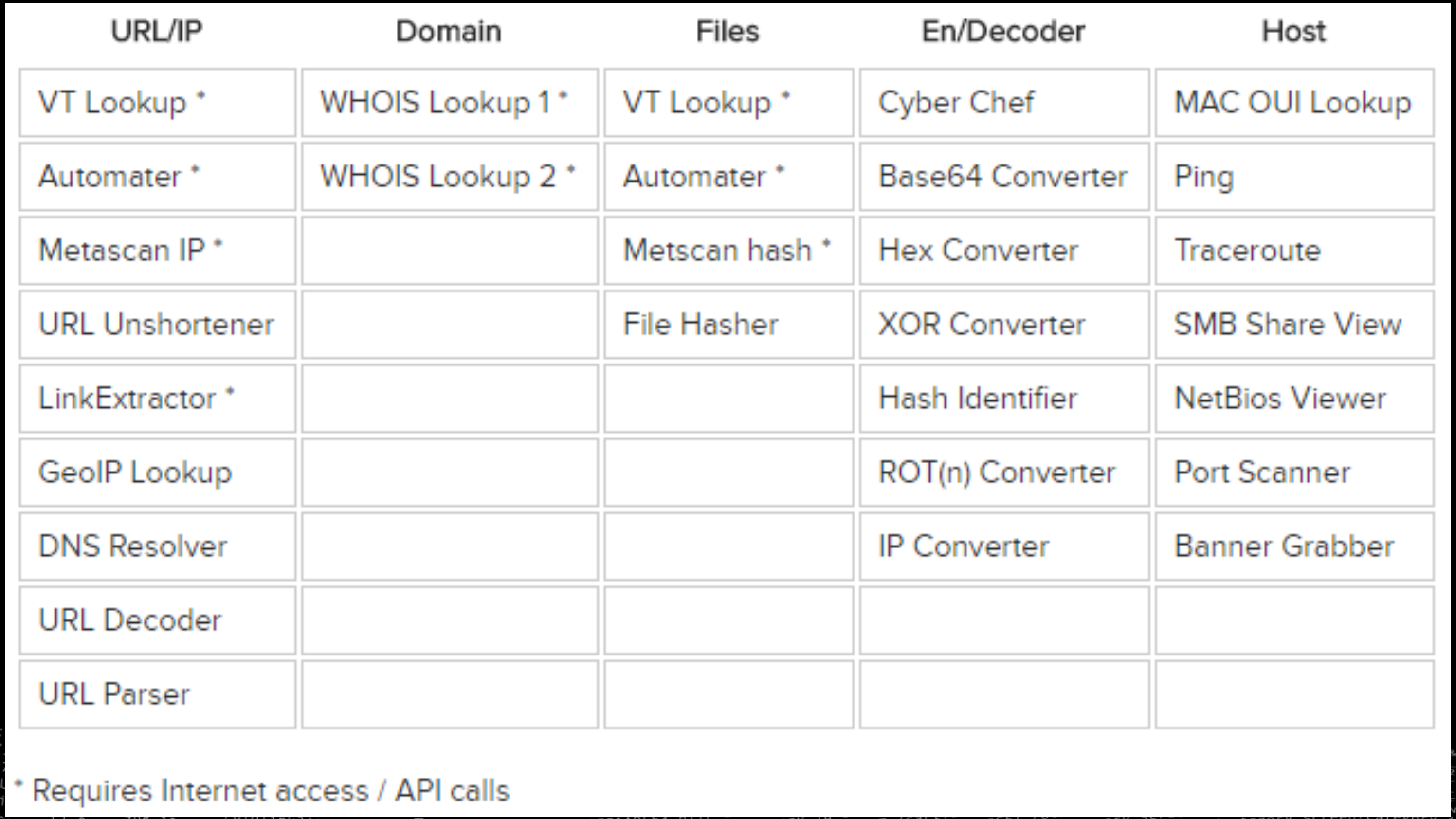
Agenda

- What Is The Forensic Investigator App?
- Design Process
- Architectural Considerations
- Handling Feedback
- Handling Updates
- Lessons Learned

What Is The Forensic Investigator App?

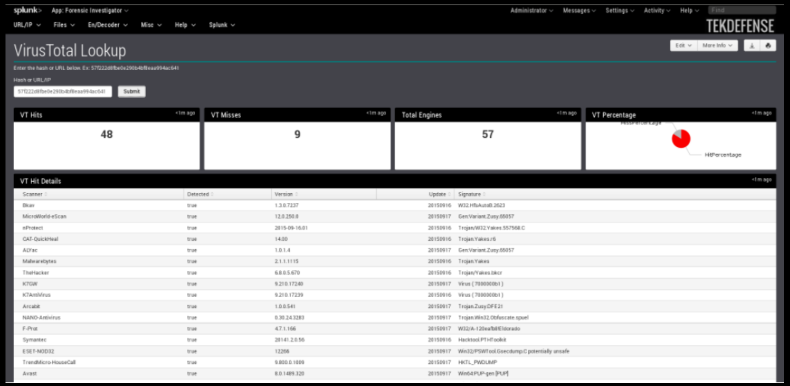
https://splunkbase.splunk.com/app/2895/

- Free Splunk app designed to assist forensic investigators / digital first responders
  - Diverse Developer backgrounds: Cylance, Splunk, DHS, Microsoft, FireEye, TekDefense
  - Loaded with tools to help investigations



URL/IP	Domain	Files	En/Decoder	Host
VT Lookup *	WHOIS Lookup 1 *	VT Lookup *	Cyber Chef	MAC OUI Lookup
Automater *	WHOIS Lookup 2 *	Automater *	Base64 Converter	Ping
Metascan IP *		Metscan hash *	Hex Converter	Traceroute
URL Unshortener		File Hasher	XOR Converter	SMB Share View
LinkExtractor *			Hash Identifier	NetBios Viewer
GeoIP Lookup			ROT(n) Converter	Port Scanner
DNS Resolver			IP Converter	Banner Grabber
URL Decoder				
URL Parser				

* Requires Internet access / API calls



splunk> App: Forensic Investigator
Administrator Messages Settings Activity Help Find
URL/IP Files En/Decoder Misc Help Splunk
TEKDEFENSE
Edit More Info
Submit
MissPercentage
HitPercentage

VirusTotal Lookup

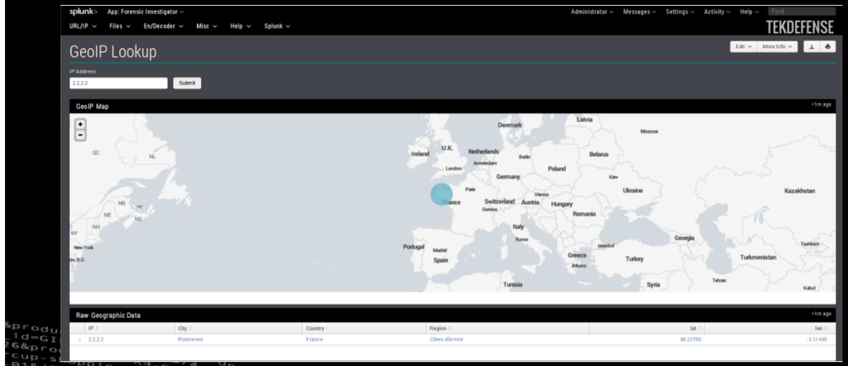
Enter the hash or URL below. Ex: 57f222d8fbe0e290b4bf8eaa994ac641

Hash or URL/IP: 57f222d8fbe0e290b4bf8eaa994ac641

VT Hits <1m ago	VT Misses <1m ago	Total Engines <1m ago	VT Percentage <1m ago
48	9	57	

VT Hit Details <1m ago

Scanner	Detected	Version	Update	Signature
Bkav	true	1.3.0.7237	20150916	W32.HfsAutoB.2623
MicroWorld-eScan	true	12.0.250.0	20150917	Gen:Variant.Zusy.65057
nProtect	true	2015-09-16.01	20150916	Trojan/W32.Yakes.557568.C
CAT-QuickHeal	true	14.00	20150916	Trojan.Yakes.r6
ALYac	true	1.0.1.4	20150917	Gen:Variant.Zusy.65057
Malwarebytes	true	2.1.1.1115	20150916	Trojan.Yakes
TheHacker	true	6.8.0.5.670	20150916	Trojan/Yakes.bkcr
K7GW	true	9.210.17240	20150917	Virus (7000000b1)
K7AntiVirus	true	9.210.17239	20150916	Virus (7000000b1)
Arcabit	true	1.0.0.541	20150917	Trojan.Zusy.DFE21
NANO-Antivirus	true	0.30.24.3283	20150917	Trojan.Win32.Obfuscate.spuel
F-Prot	true	4.7.1.166	20150917	W32/A-120eafb8!Eldorado
Symantec	true	20141.2.0.56	20150916	Hacktool.PTHToolkit
ESET-NOD32	true	12266	20150917	Win32/PSWTool.Gsecdump.C potentially unsafe
TrendMicro-HouseCall	true	9.800.0.1009	20150917	HKTL_PWDUMP
Avast	true	8.0.1489.320	20150917	Win64:PUP-gen [PUP]



GeoIP Lookup

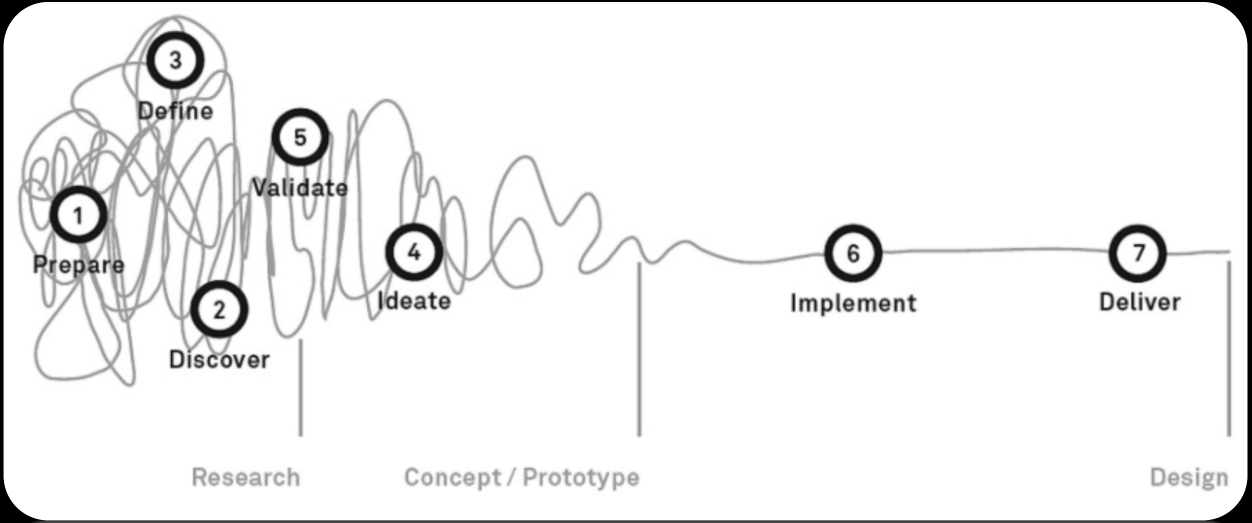
IP Address: 2.2.2.2

Raw Geographic Data <1m ago

	IP	City	Country	Region	lat	lon
1	2.2.2.2	Rostrenen	France	Côtes-d'Armor	48.23700	-3.31440

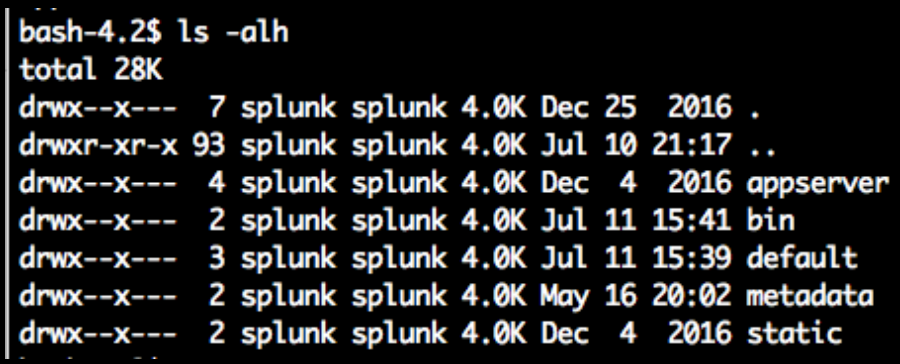
Design Process

- Take time at the start to avoid pitfalls
  - App, Index, and sourcetype names
    - Examples: alerts, fi:alerts, fi:alerts:syslog
  - Inputs
    - Enable everything?
  - Eventtypes
    - Use them early
      - eventtype=fi_index
  - Admin required functions



Design Process (Cont’d)

- Fast & Frequent Iterations
  - Quick and Dirty is OK
    - | script vtlookup __EXECUTE__ "$search_hash_url$"
  - Work towards standardization over time
    - Most tech debt has proven nominal



```
bash-4.2$ ls -alh
total 28K
drwx--x---  7 splunk splunk 4.0K Dec 25  2016 .
drwxr-xr-x 93 splunk splunk 4.0K Jul 10 21:17 ..
drwx--x---  4 splunk splunk 4.0K Dec  4  2016 appserver
drwx--x---  2 splunk splunk 4.0K Jul 11 15:41 bin
drwx--x---  3 splunk splunk 4.0K Jul 11 15:39 default
drwx--x---  2 splunk splunk 4.0K May 16 20:02 metadata
drwx--x---  2 splunk splunk 4.0K Dec  4  2016 static
```

- Change Has Consequences
  - App Certification doesn’t like many small updates
  - One small change may have huge consequences for large install bases
  - Change for the sake of change is often bad

Architectural Considerations

- How will your users install and use the app?
  - App + TA
    - Search head vs. indexer vs. forwarder?
  - Splunk on Windows or Nix?
    - Paths matter (ex: $SPLUNK_HOME?)
  - Cloud vs. on-prem
    - Editing configuration files
  - Proxy aware
    - Passing lots of secrets via GET?

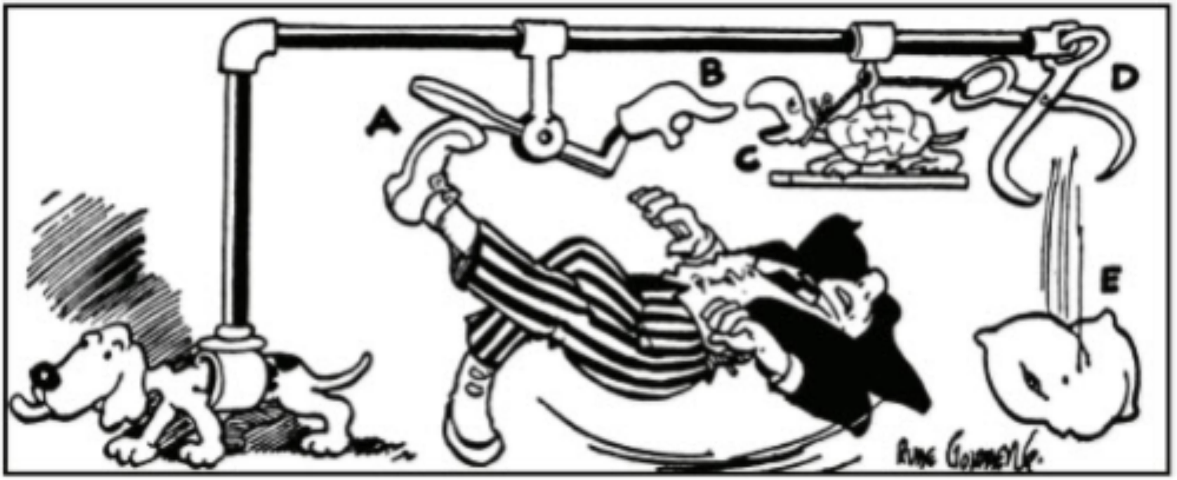


Figure 1. Safety device for walking on icy pavements: when you slip on ice your foot kicks paddle (A), lowering finger (B), snapping turtle (C) extends neck to bite finger opening ice tongs (D) and dropping pillow (E), thus allowing you to fall on something soft. (Rube Goldberg Inc., n.d.)

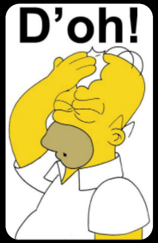
Handling Feedback

- Feedback Is Great! (most of the time)
  - Mechanism
    - Email link within the app
    - Splunk Answers
  - Great ideas
    - Your users may have awesome ideas
    - Let them help drive the road map
  - Narrow focus
    - Be careful to not be consumed with user ideas – they may not be best for the whole

Handling Updates

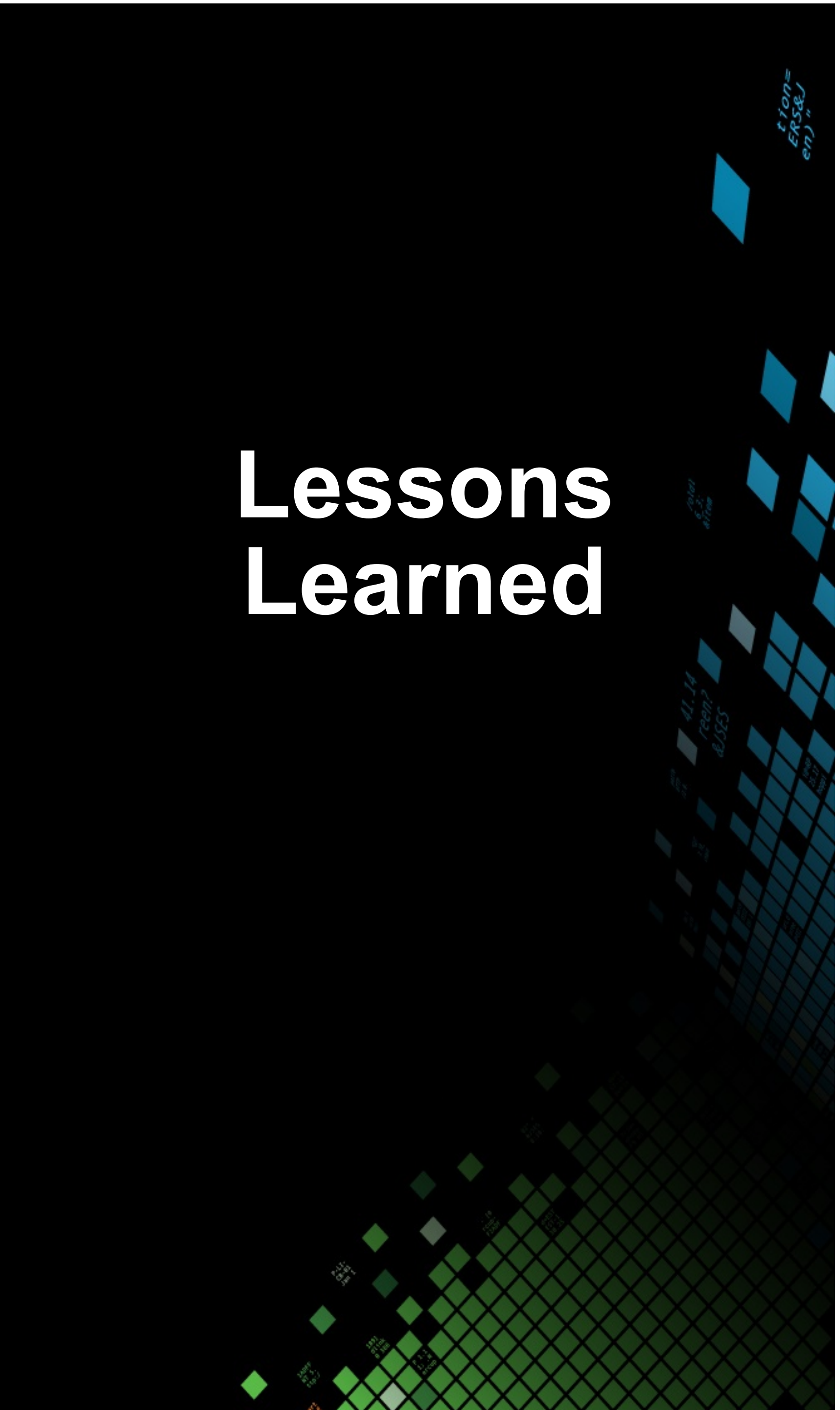
- Rule #1 - Don’t break anything
  - User’s environment
    - Saved searches
    - Parsing inefficiencies

  - Your own app
    - Installation failure
    - Collisions on Setup



  - Your user’s custom dashboards
    - Changing index and sourcetype names

- Rule #2 – See rule #1



Lessons Learned

1. Spend a little time in design – pays dividends

2. Think about how people will install and use the app

3. Have a diverse development team / board of advisers

4. Handle feedback gracefully

5. Don’t break anything (best effort)

6. Don’t be afraid to publish your own app

Thank You

Don't forget to rate this session in the .conf2017 mobile app

splunk> .conf2017