RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking

SESSION ID: TECH-T10

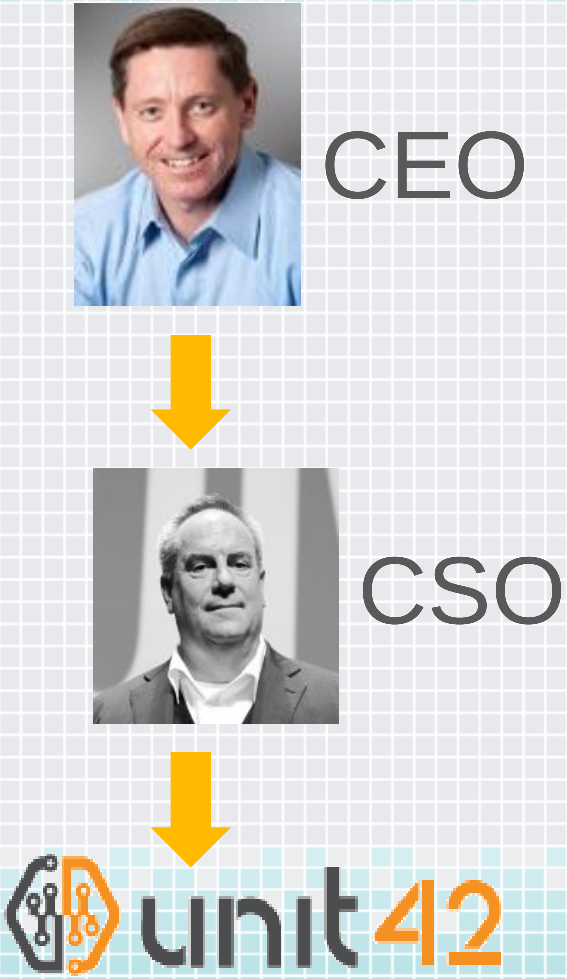
Powering Your Threat Intel Team with Off-the-Shelf Tools

Ryan Olson

Intelligence Director
Palo Alto Networks
@ireo

/usr/bin/whoami

Mission: Analyze the data available to Palo Alto Networks to identify adversaries, their motivations and resources to better understand the threats our customers face.



CEO

CSO

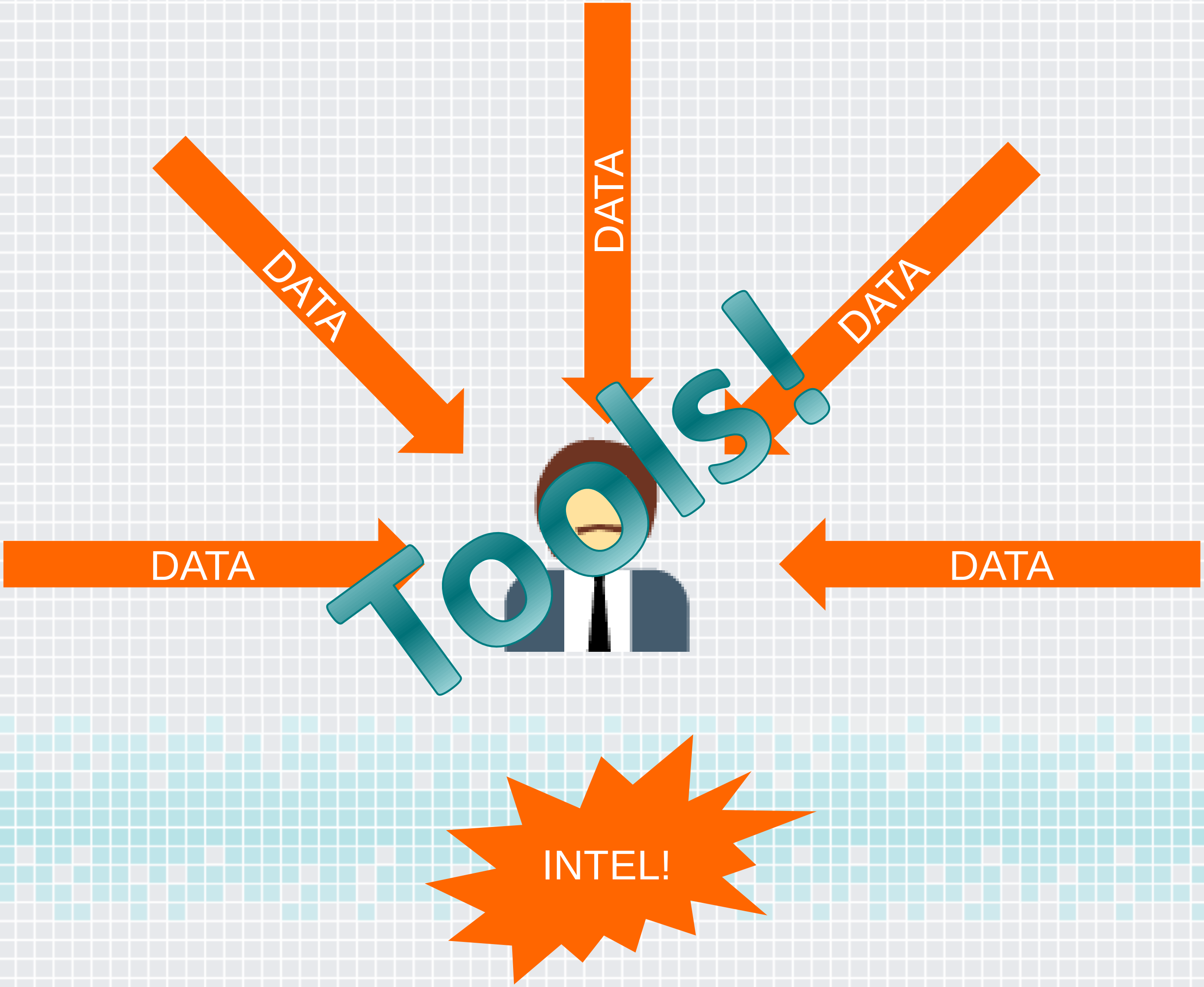
What is Threat Intelligence?

"Evidence-based knowledge, including **context**, mechanisms, indicators, implications and **actionable** advice, about an existing or emerging menace or hazard to assets that can be used to **inform decisions** regarding the subject's response to that menace or hazard."

- Rob McMillan - Gartner

212.83.131.214 is Bad ✗

On May 6, 2014, 212.83.131.214 hosted a command and control server for the NetWire RAT on TCP port 3360 in association with an attack from Nigerian cyber criminals… ✓



DATA

DATA

DATA

DATA

DATA

Tools!

INTEL!

Which Tools?

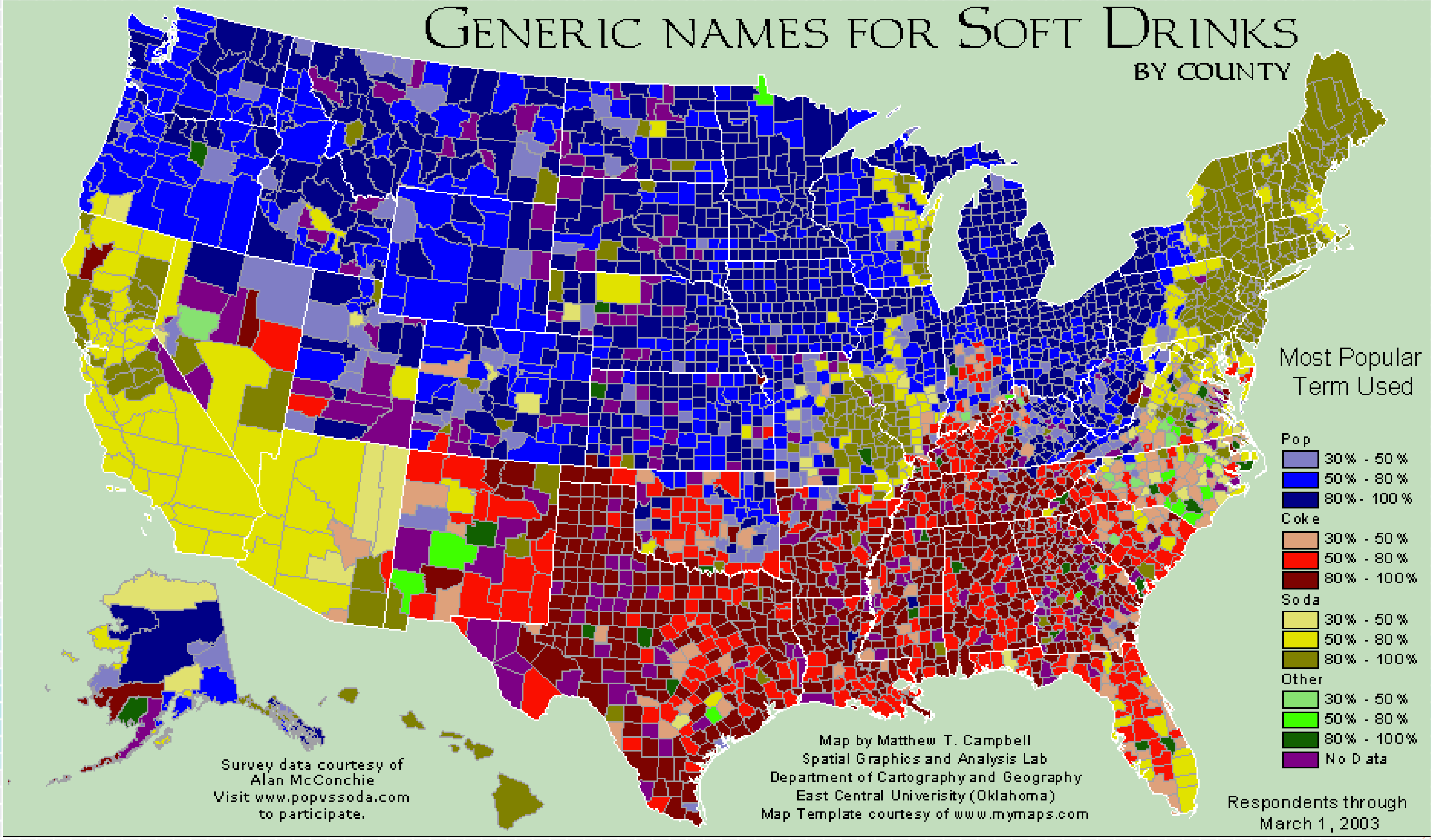
- No Data Sinkholes
  - Data that goes in, must come out.
- Extensible – Add our own functionality
  - Without $$$ consulting bills…
- Active Community
  - Easier to trouble-shoot
  - Faster feature development
  - Easier to find staff familiar with the tool chain.

Tools

Visualization

Intel Repository &
Work Bench

Why Visualize Data



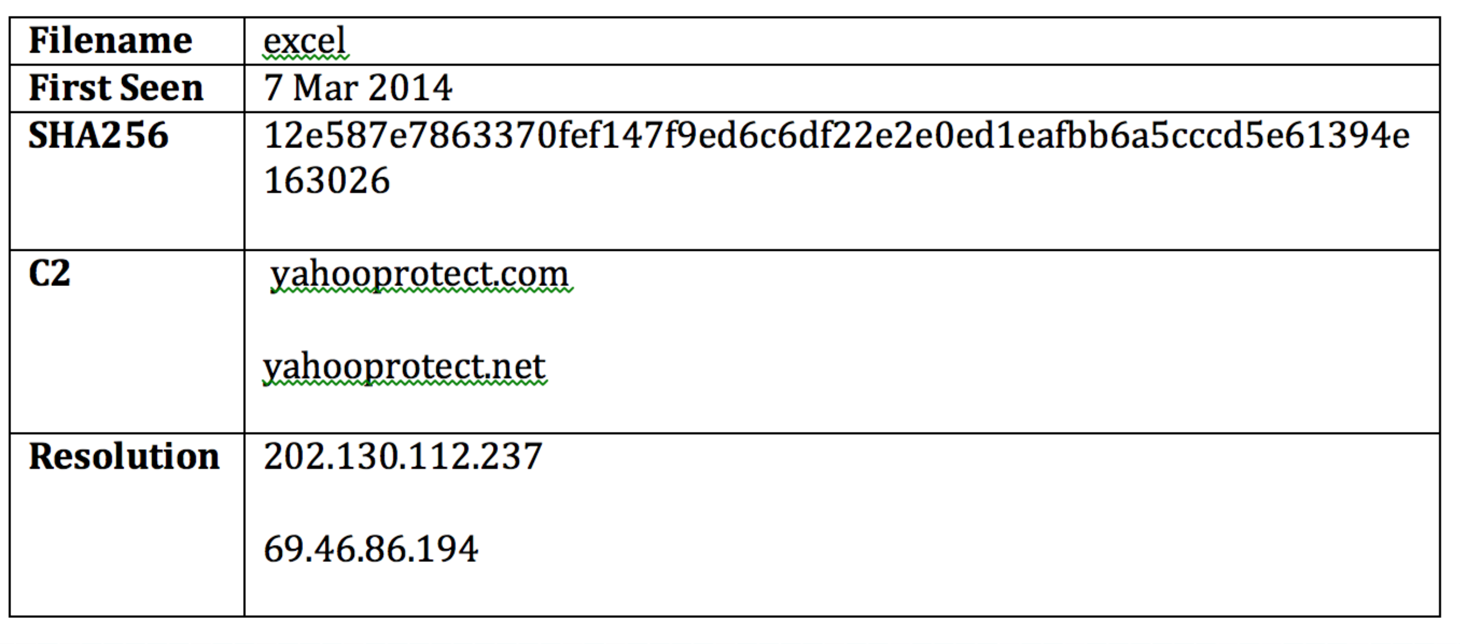
GENERIC NAMES FOR SOFT DRINKS
BY COUNTY

Survey data courtesy of
Alan McConchie
Visit www.popvssoda.com
to participate.

Map by Matthew T. Campbell
Spatial Graphics and Analysis Lab
Department of Cartography and Geography
East Central Univerisity (Oklahoma)
Map Template courtesy of www.mymaps.com

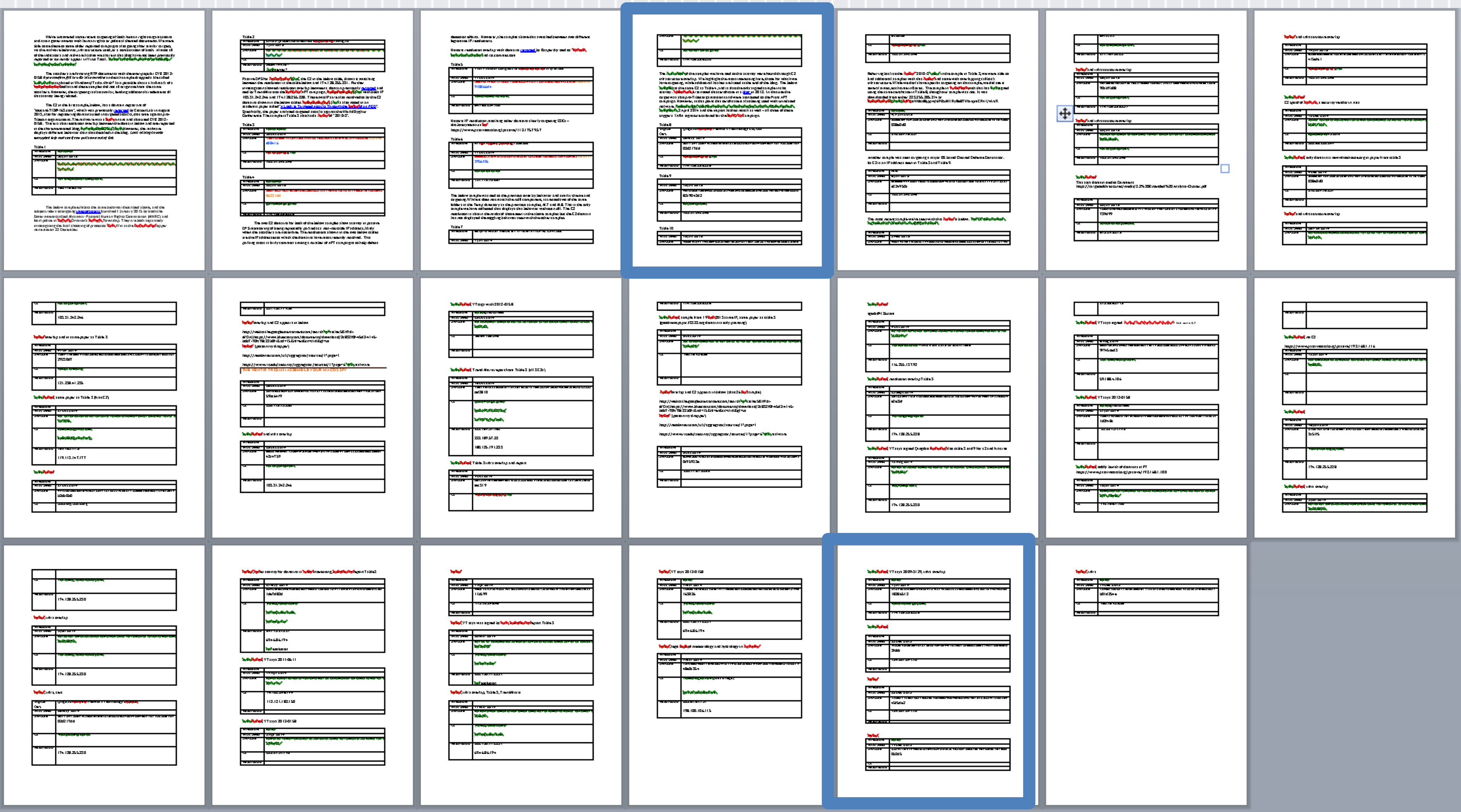
Respondents through
March 1, 2003

Typical Data Points

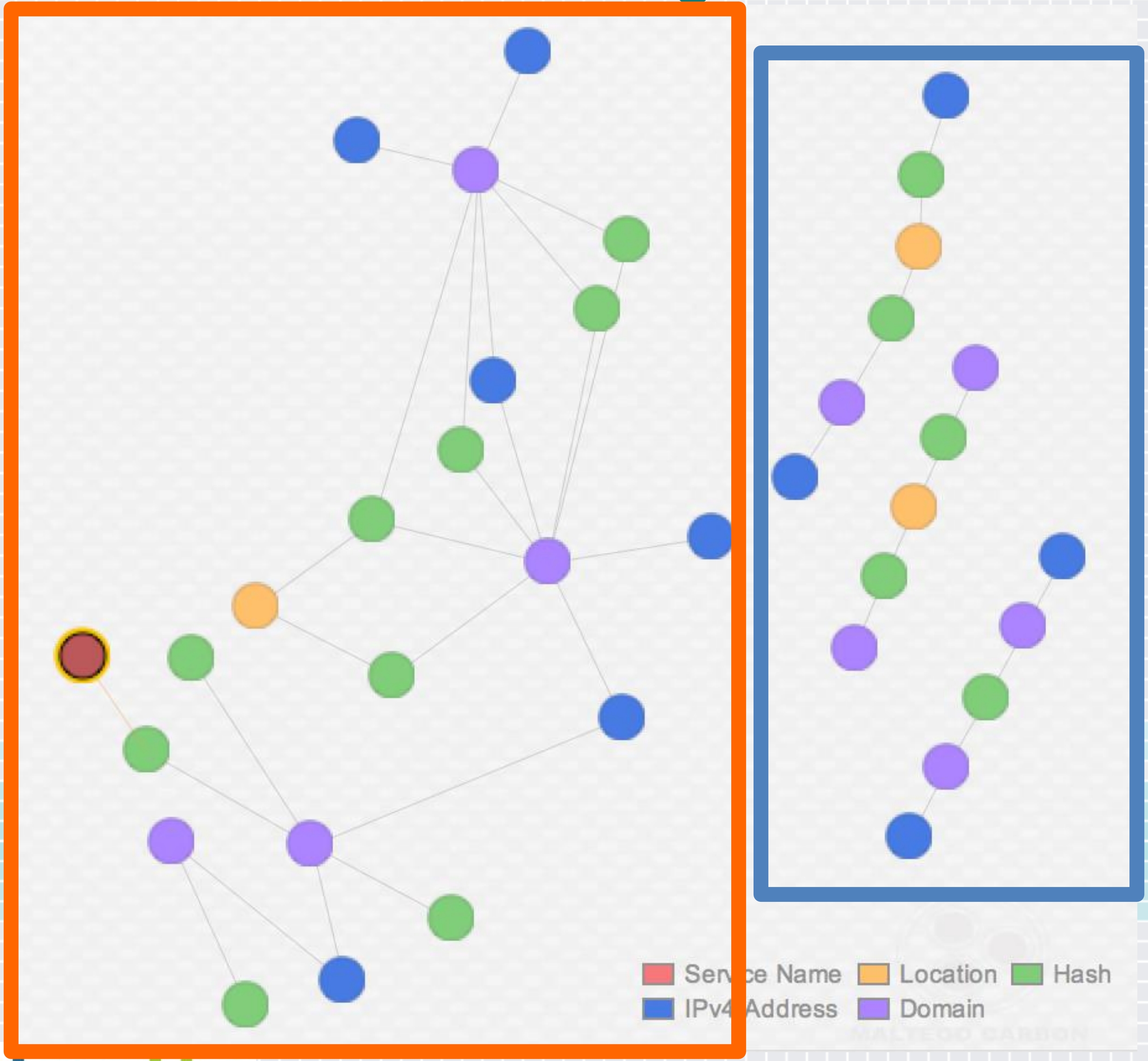


Filename	excel
First Seen	7 Mar 2014
SHA256	12e587e7863370fef147f9ed6c6df22e2e0ed1eafbb6a5cccd5e61394e163026
C2	yahooprotect.com yahooprotect.net
Resolution	202.130.112.237 69.46.86.194

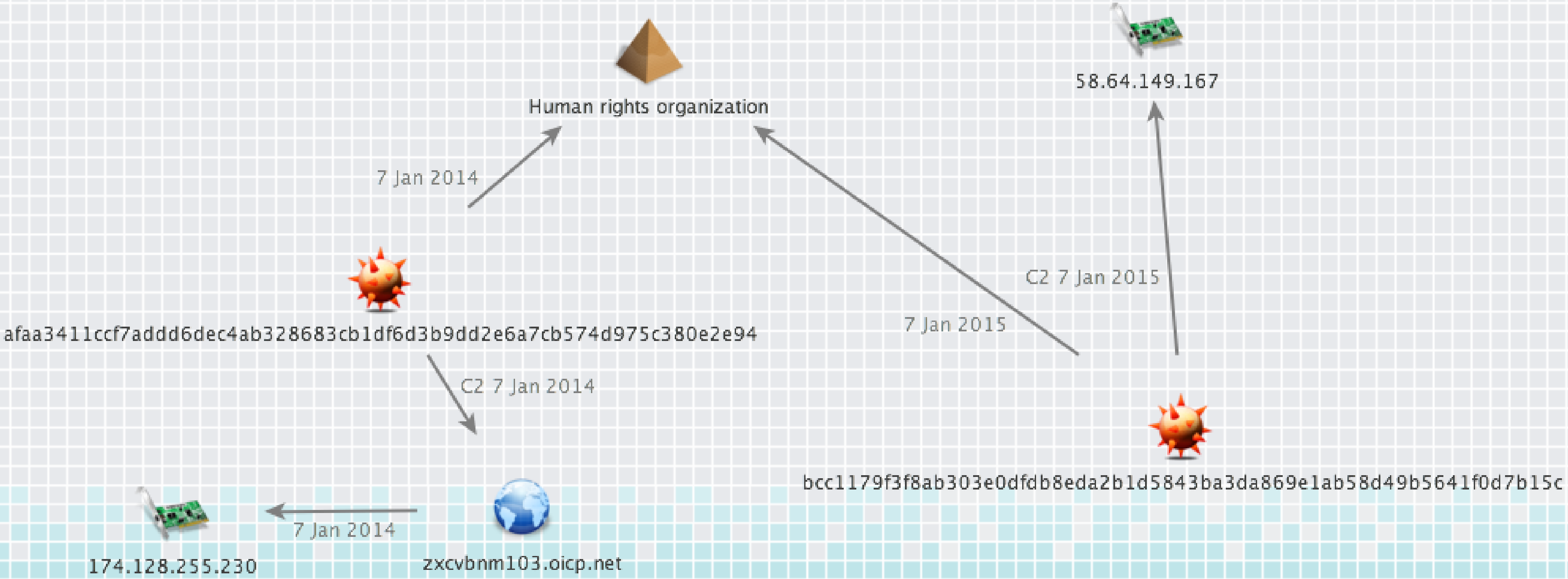
20 Pages of Notes



Notes Visualized In Maltego

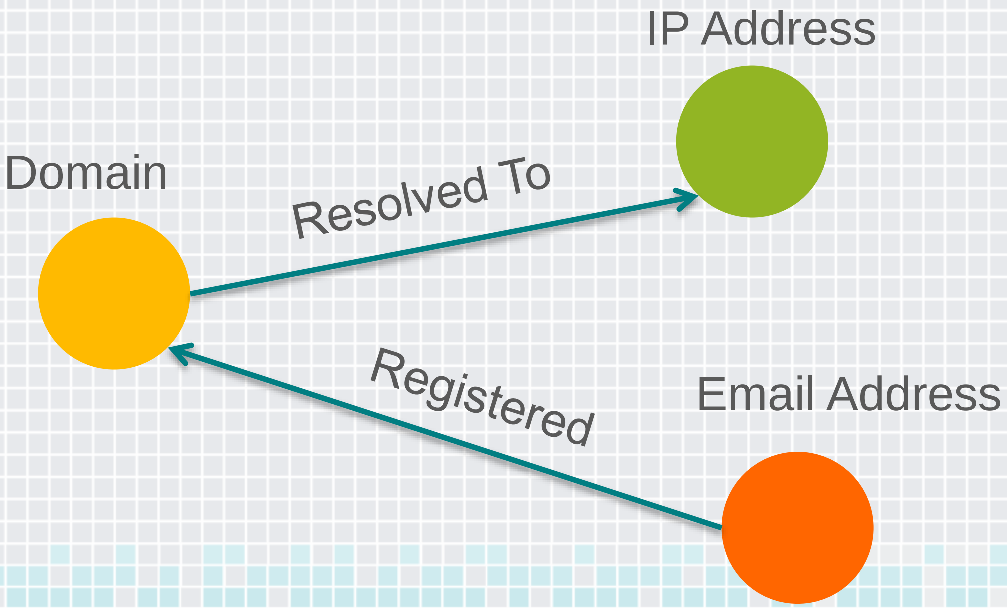


Notes Visualized in Maltego

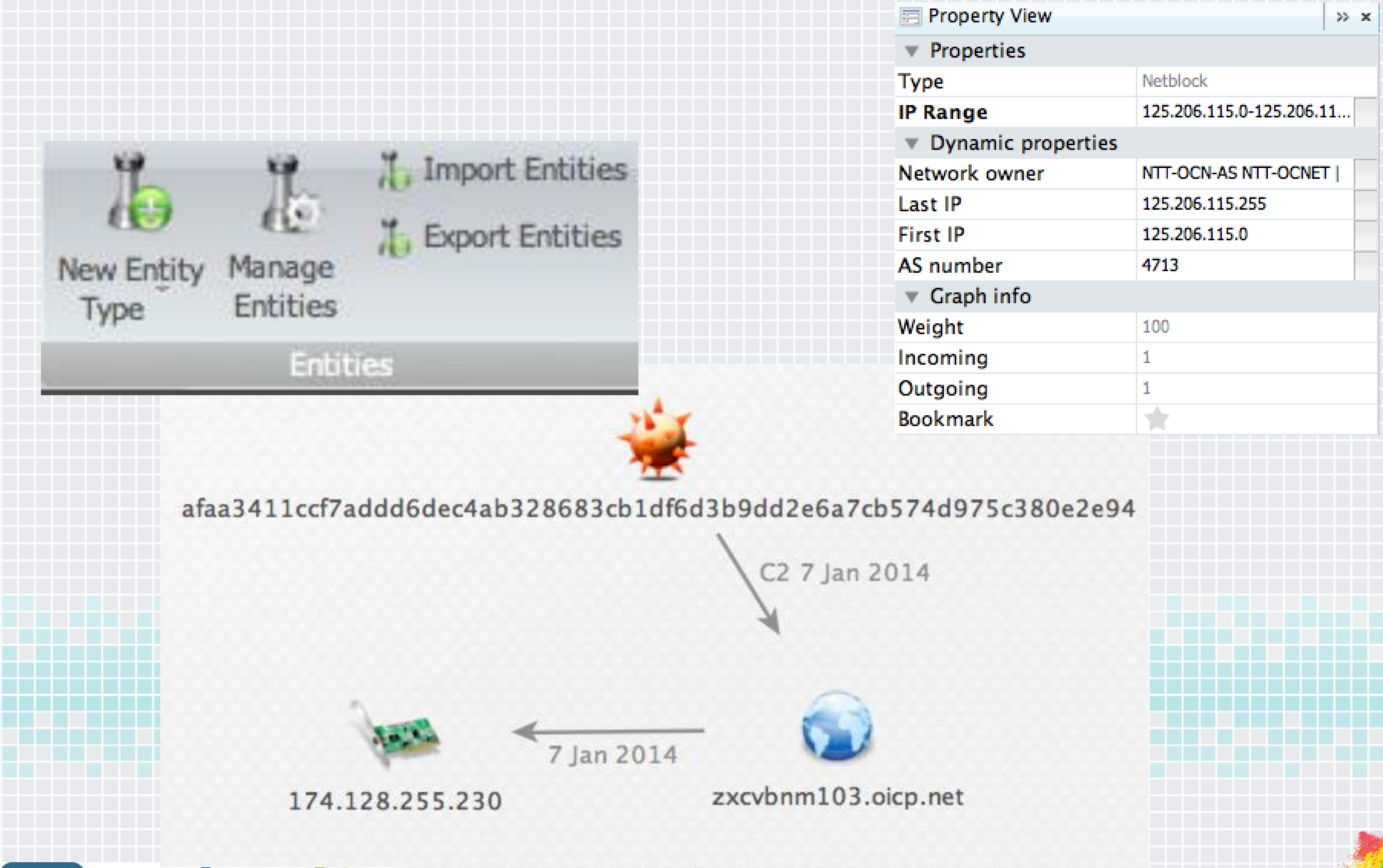

Human rights organization
58.64.149.167
7 Jan 2014
C2 7 Jan 2015
7 Jan 2015
afaa3411ccf7addd6dec4ab328683cb1df6d3b9dd2e6a7cb574d975c380e2e94
C2 7 Jan 2014
bcc1179f3f8ab303e0dfdb8eda2b1d5843ba3da869e1ab58d49b5641f0d7b15c
7 Jan 2014
174.128.255.230
zxcvbnm103.oicp.net

Why Maltego?

Maltego Concepts: Entities and Links



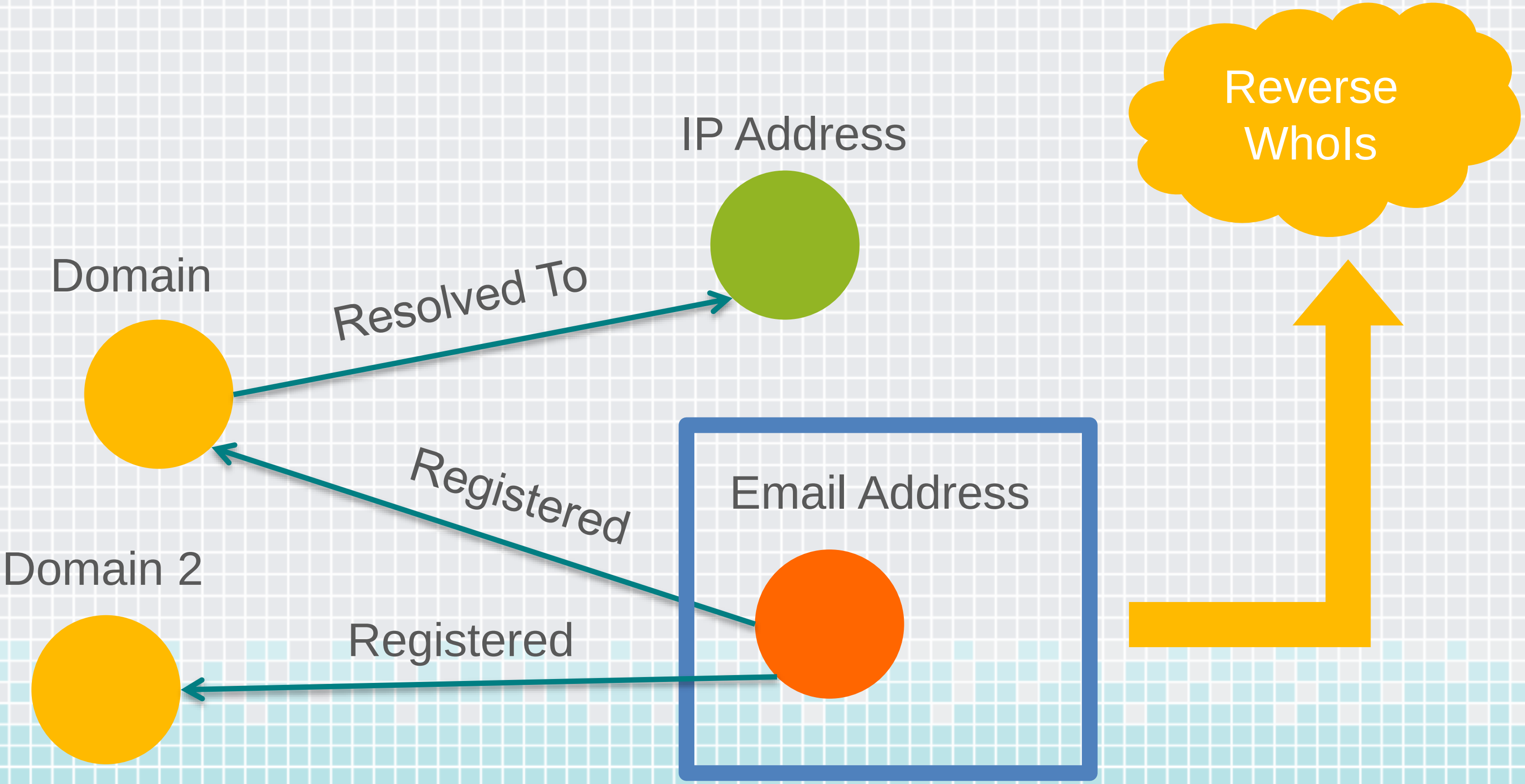
Maltego Concepts: Entities and Links



Property View

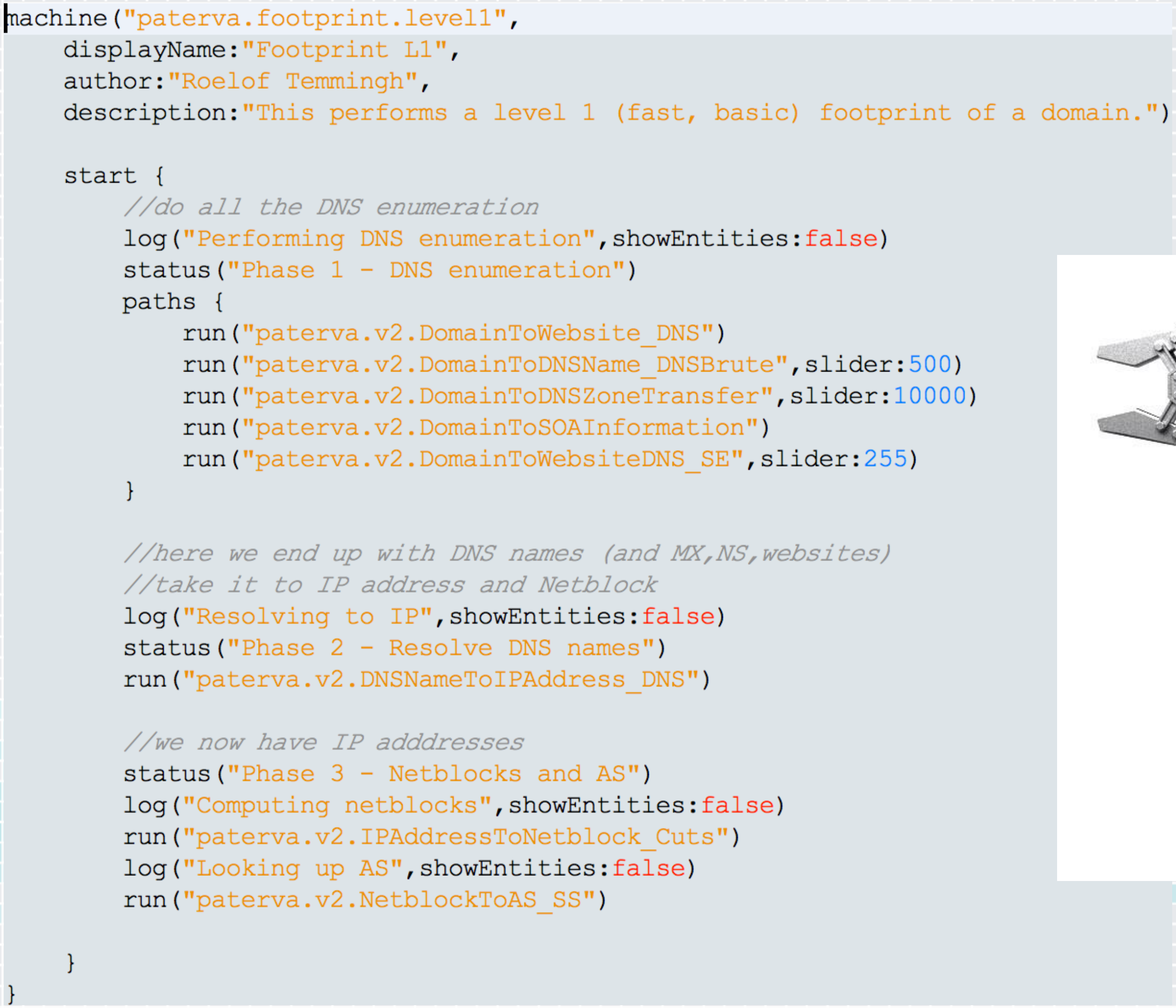
Properties	
Type	Netblock
IP Range	125.206.115.0-125.206.11...
Dynamic properties	
Network owner	NTT-OCN-AS NTT-OCNET |
Last IP	125.206.115.255
First IP	125.206.115.0
AS number	4713
Graph info	
Weight	100
Incoming	1
Outgoing	1
Bookmark	☆

Maltego Concepts: Transforms



Maltego Demo

Maltego Concepts: Machines



```
machine("paterva.footprint.level1",
    displayName:"Footprint L1",
    author:"Roelof Temmingh",
    description:"This performs a level 1 (fast, basic) footprint of a domain.")

    start {
        //do all the DNS enumeration
        log("Performing DNS enumeration",showEntities:false)
        status("Phase 1 - DNS enumeration")
        paths {
            run("paterva.v2.DomainToWebsite_DNS")
            run("paterva.v2.DomainToDNSName_DNSBrute",slider:500)
            run("paterva.v2.DomainToDNSZoneTransfer",slider:10000)
            run("paterva.v2.DomainToSOAInformation")
            run("paterva.v2.DomainToWebsiteDNS_SE",slider:255)
        }

        //here we end up with DNS names (and MX,NS,websites)
        //take it to IP address and Netblock
        log("Resolving to IP",showEntities:false)
        status("Phase 2 - Resolve DNS names")
        run("paterva.v2.DNSNameToIPAddress_DNS")

        //we now have IP adddresses
        status("Phase 3 - Netblocks and AS")
        log("Computing netblocks",showEntities:false)
        run("paterva.v2.IPAddressToNetblock_Cuts")
        log("Looking up AS",showEntities:false)
        run("paterva.v2.NetblockToAS_SS")

    }
}
```

Outside Data Sources

DomainTools

THREATCONNECT
Driven by community. Defined by intelligence.

SHODAN

INTERNET STORM CENTER

virustotal

Recorded Future
CREATING AN INSIGHTFUL WORLD

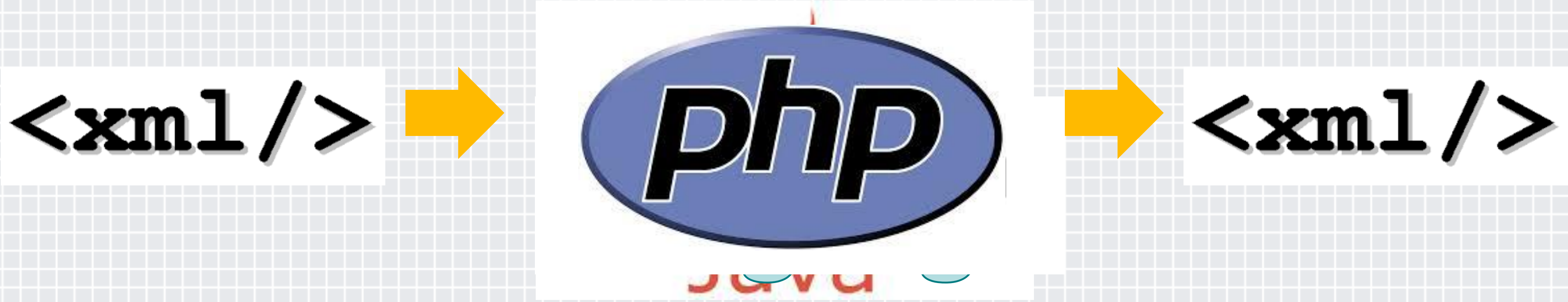
CALAIS
Powered by Thomson Reuters

Threat Expert

PassiveTotal

paloalto NETWORKS

Connecting Your Own Data



Local VS Remote

Local Transforms

- Run from the local system
- Pros:
  - Quick to setup, prototype
  - Data is private
- Cons
  - Difficult to distribute, all users need to have all require software
  - Difficult to Update
  - Fewer Settings

Remote Transforms

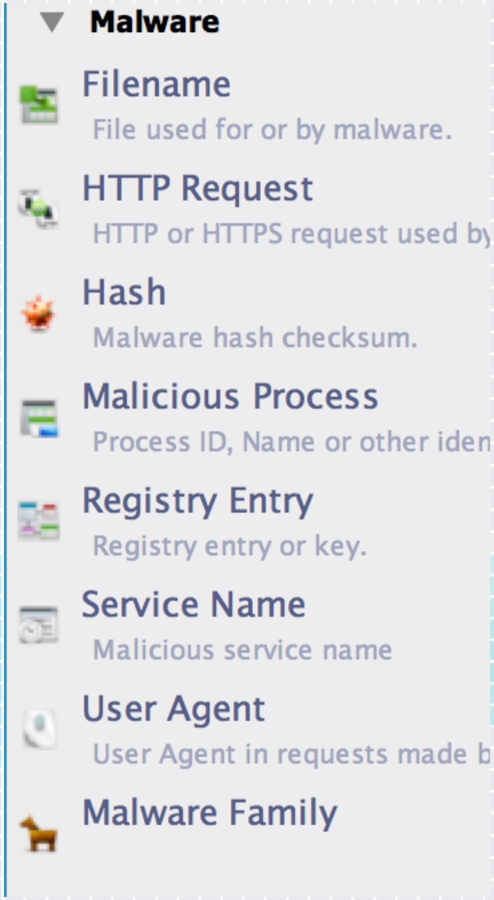
- Run from a Transform Distribution Server (TDS)
- Pros:
  - Very easy to share with others.
  - Single point of updates/configuration.
  - Ability to rate limit users.
  - Best for teams and services.
- Cons:
  - Data sent to public servers
  - Can be private (but expensive)

Libraries

- You could write pure XML…
- Python
  - PyMaltego
  - Basic Python Library (Paterva)
  - Canari
- Canari is by far the best option for local development.
  - Abstracts all XML
  - Handles Entities
  - Creates distributable bundles
  - But…local system still needs software installed.

MALFORMITYLABS

- Malware Related Entities + Transforms
- Local execution
- Built with Canari



▼ **Malware**

Filename
File used for or by malware.

HTTP Request
HTTP or HTTPS request used by

Hash
Malware hash checksum.

Malicious Process
Process ID, Name or other iden

Registry Entry
Registry entry or key.

Service Name
Malicious service name

User Agent
User Agent in requests made b

Malware Family

Where's Your Intelligence Stored?

E-MAIL?

SEIM?

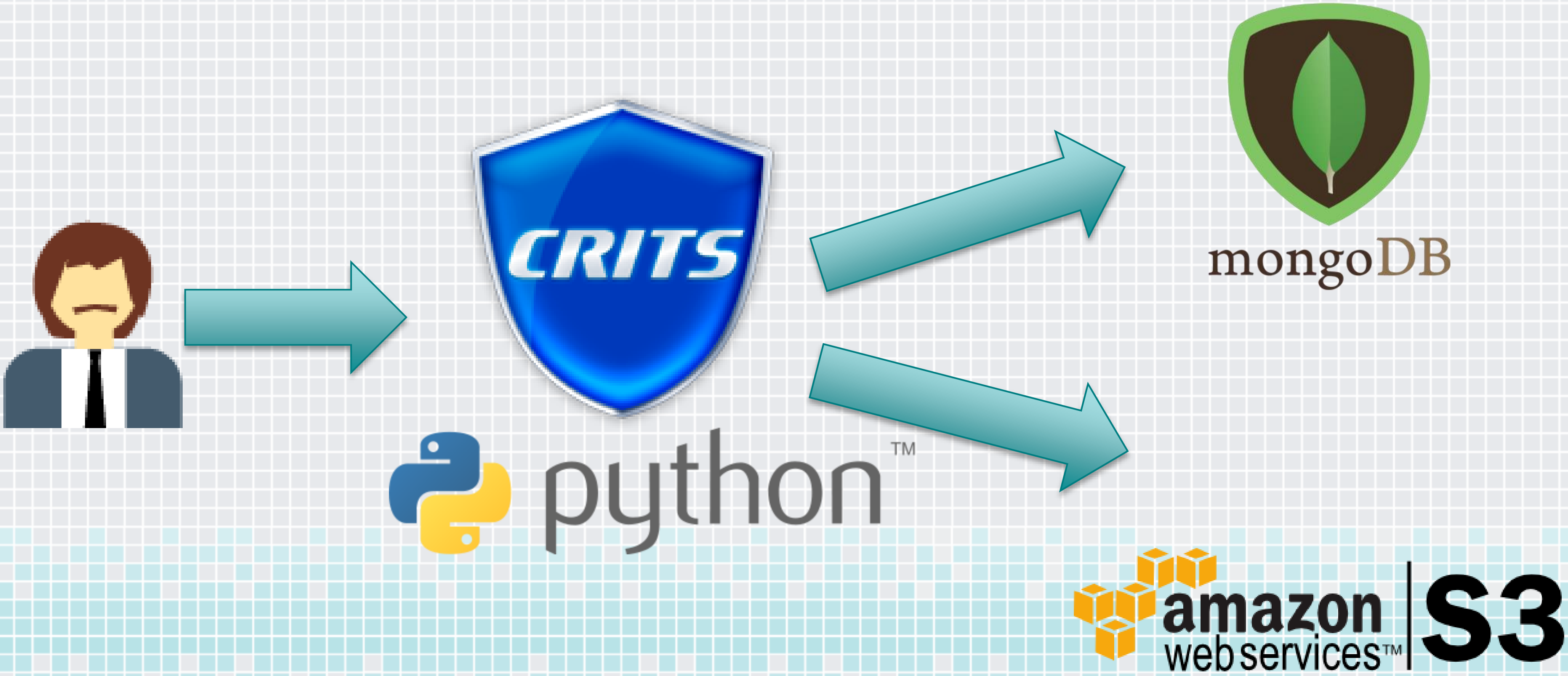
DOC?

PDF?

XLS?

BRAIN?

Collaborative Research Into Threats (CRITs)



Why CRITs?

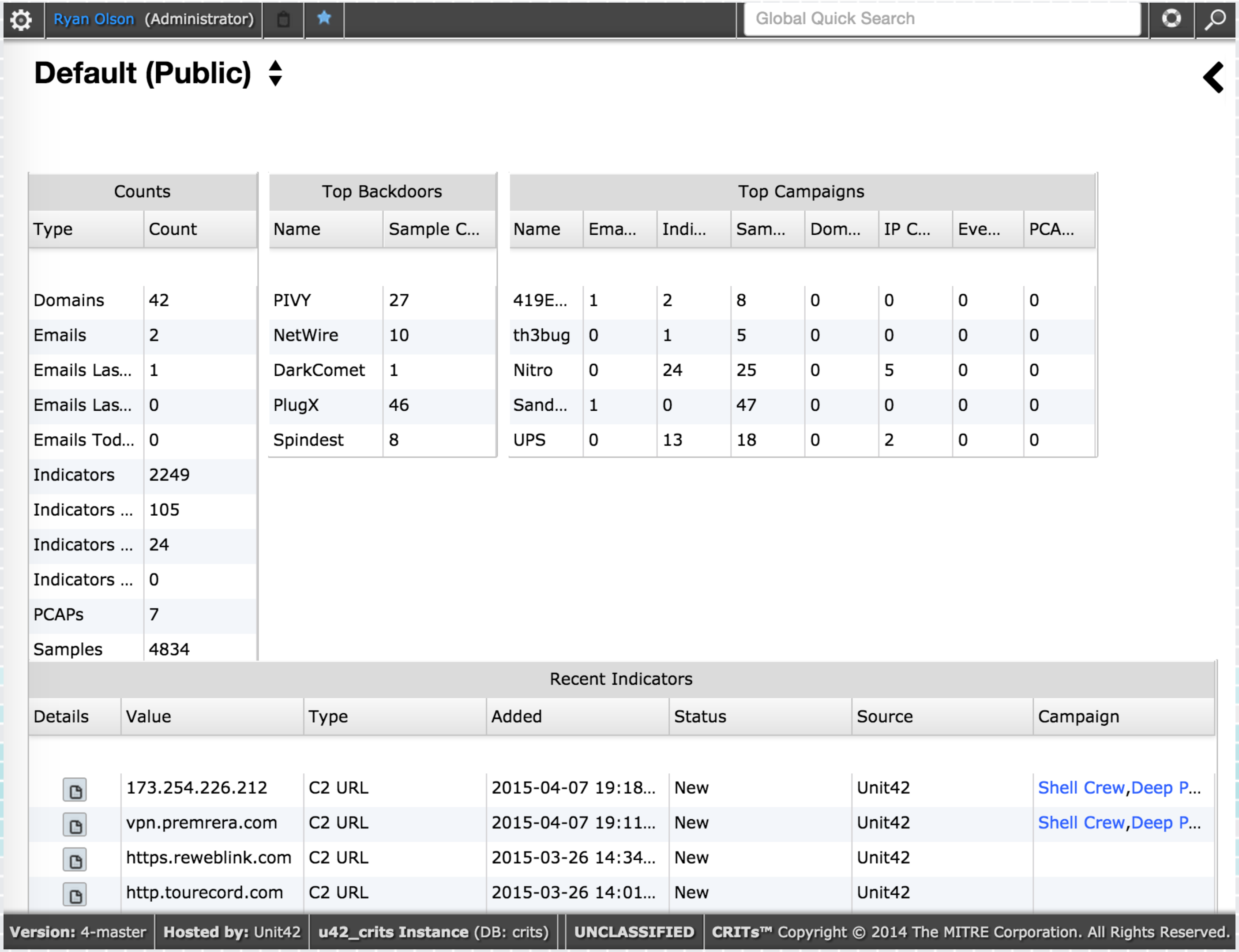
Top Level Objects

- Actors
- Campaigns
- Certificates
- Domains
- Emails
- Events
- Indicators
- IPs
- PCAP
- Raw Data
- Samples
- Targets

Concepts

- Bucket Lists
- Campaign Attribution
- Comments
- Downloading
- Email Targets
- Favorites
- Notifications
- Objects
- Relationships
- Releasability
- Screenshots
- Sectors
- Sources
- Subscriptions

CRITs Dashboard



Ryan Olson (Administrator)

Global Quick Search

Default (Public)

Counts	
Type	Count
Domains	42
Emails	2
Emails Las...	1
Emails Las...	0
Emails Tod...	0
Indicators	2249
Indicators ...	105
Indicators ...	24
Indicators ...	0
PCAPs	7
Samples	4834

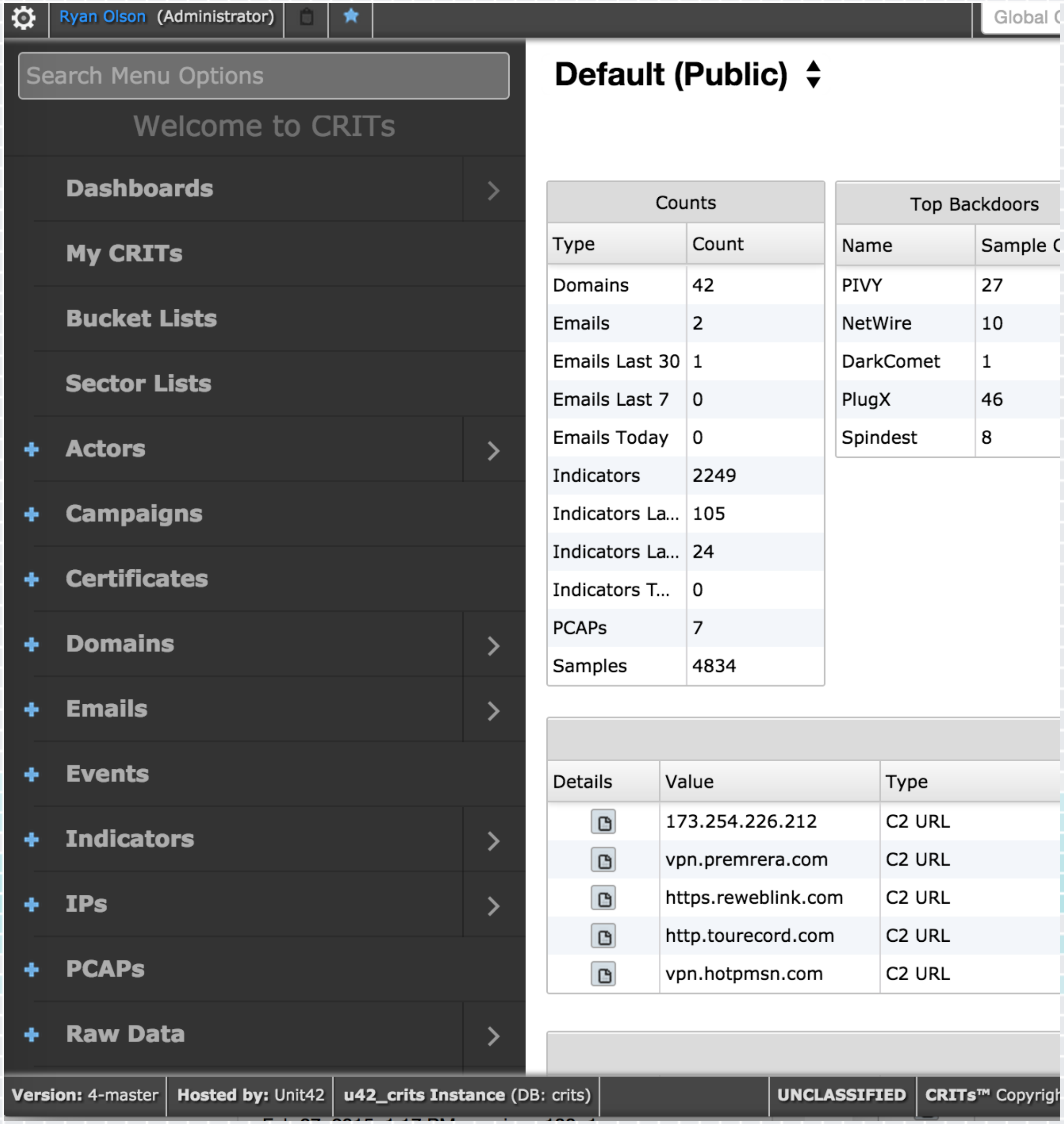
Top Backdoors	
Name	Sample C...
PIVY	27
NetWire	10
DarkComet	1
PlugX	46
Spindest	8

Top Campaigns							
Name	Ema...	Indi...	Sam...	Dom...	IP C...	Eve...	PCA...
419E...	1	2	8	0	0	0	0
th3bug	0	1	5	0	0	0	0
Nitro	0	24	25	0	5	0	0
Sand...	1	0	47	0	0	0	0
UPS	0	13	18	0	2	0	0

Recent Indicators						
Details	Value	Type	Added	Status	Source	Campaign
🗎	173.254.226.212	C2 URL	2015-04-07 19:18...	New	Unit42	Shell Crew,Deep P...
🗎	vpn.premrera.com	C2 URL	2015-04-07 19:11...	New	Unit42	Shell Crew,Deep P...
🗎	https.reweblink.com	C2 URL	2015-03-26 14:34...	New	Unit42	
🗎	http.tourecord.com	C2 URL	2015-03-26 14:01...	New	Unit42	

Version: 4-master | **Hosted by:** Unit42 | **u42_crits Instance** (DB: crits) | **UNCLASSIFIED** | **CRITs™** Copyright © 2014 The MITRE Corporation. All Rights Reserved.

CRITs Menu



Ryan Olson (Administrator)

Global (

Search Menu Options

Welcome to CRITs

- Dashboards
- My CRITs
- Bucket Lists
- Sector Lists
- + Actors
- + Campaigns
- + Certificates
- + Domains
- + Emails
- + Events
- + Indicators
- + IPs
- + PCAPs
- + Raw Data

Default (Public)

Counts

Type	Count
Domains	42
Emails	2
Emails Last 30	1
Emails Last 7	0
Emails Today	0
Indicators	2249
Indicators La...	105
Indicators La...	24
Indicators T...	0
PCAPs	7
Samples	4834

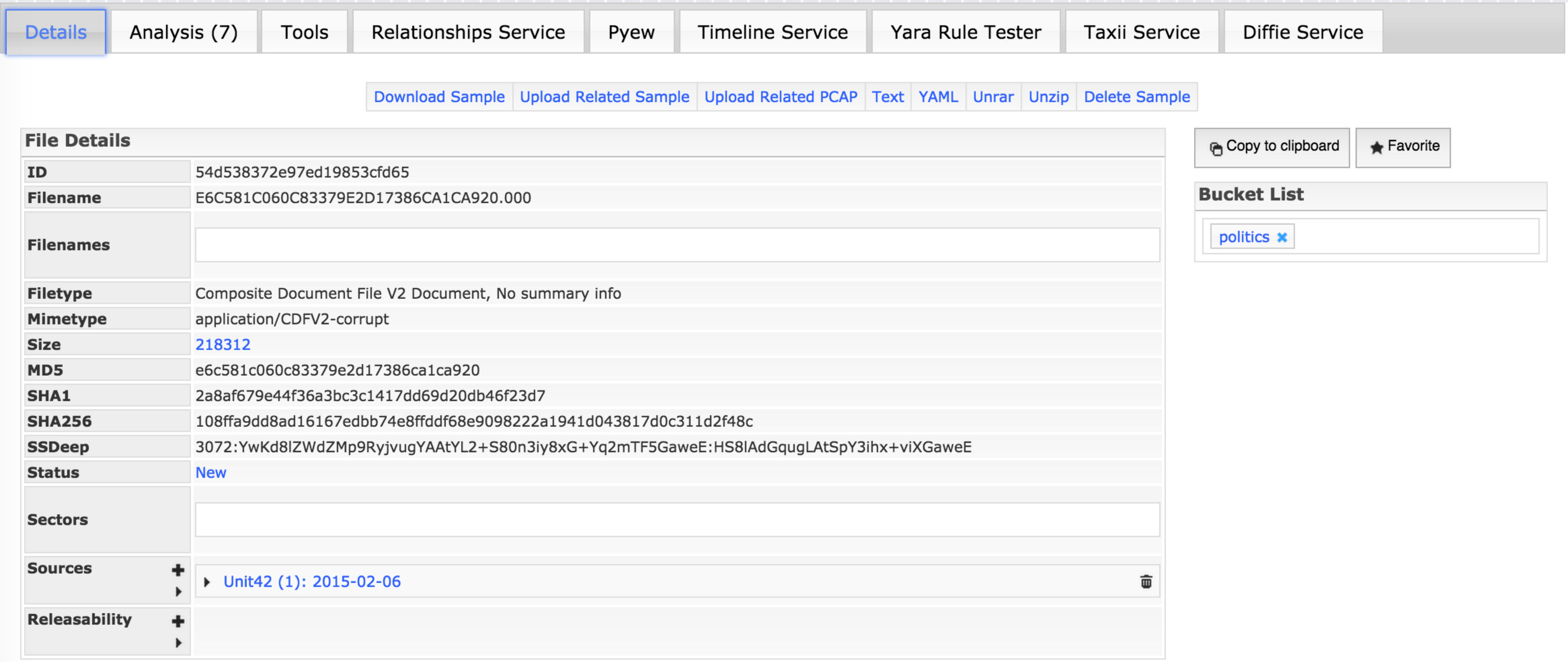
Top Backdoors

Name	Sample C
PIVY	27
NetWire	10
DarkComet	1
PlugX	46
Spindest	8

Details	Value	Type
🗋	173.254.226.212	C2 URL
🗋	vpn.premrera.com	C2 URL
🗋	https.reweblink.com	C2 URL
🗋	http.tourecord.com	C2 URL
🗋	vpn.hotpmsn.com	C2 URL

Version: 4-master | **Hosted by:** Unit42 | **u42_crits Instance** (DB: crits) | **UNCLASSIFIED** | **CRITs™** Copyrigh

CRITs Object Details



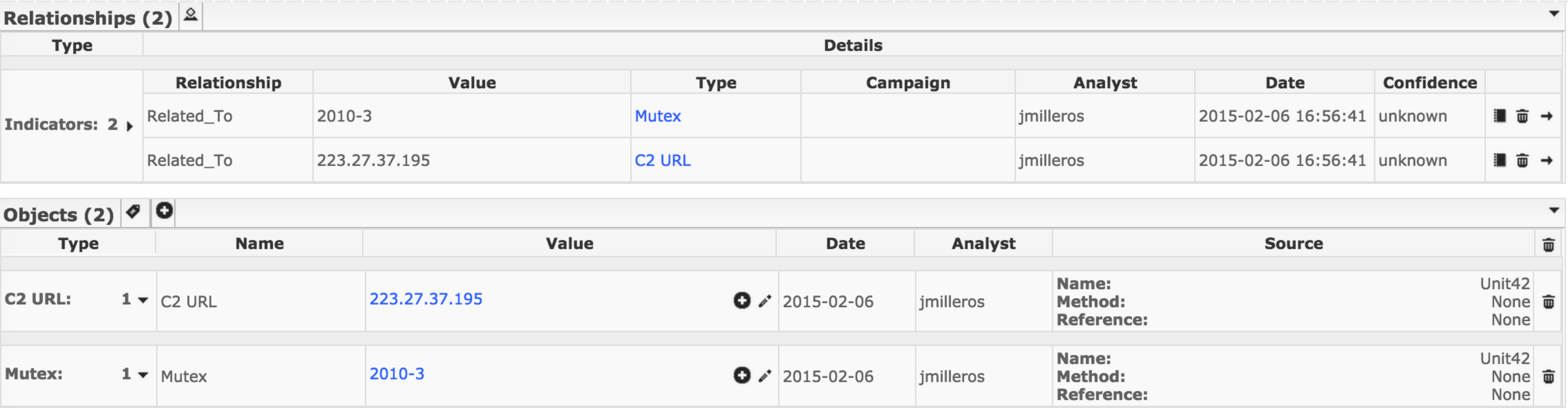
File Details

ID	54d538372e97ed19853cfd65
Filename	E6C581C060C83379E2D17386CA1CA920.000
Filenames	
Filetype	Composite Document File V2 Document, No summary info
Mimetype	application/CDFV2-corrupt
Size	218312
MD5	e6c581c060c83379e2d17386ca1ca920
SHA1	2a8af679e44f36a3bc3c1417dd69d20db46f23d7
SHA256	108ffa9dd8ad16167edbb74e8ffddf68e9098222a1941d043817d0c311d2f48c
SSDeep	3072:YwKd8lZWdZMp9RyjvugYAAtYL2+S80n3iy8xG+Yq2mTF5GaweE:HS8lAdGqugLAtSpY3ihx+viXGaweE
Status	New
Sectors	
Sources	Unit42 (1): 2015-02-06
Releasability	

Bucket List

politics

CRITs Relationships



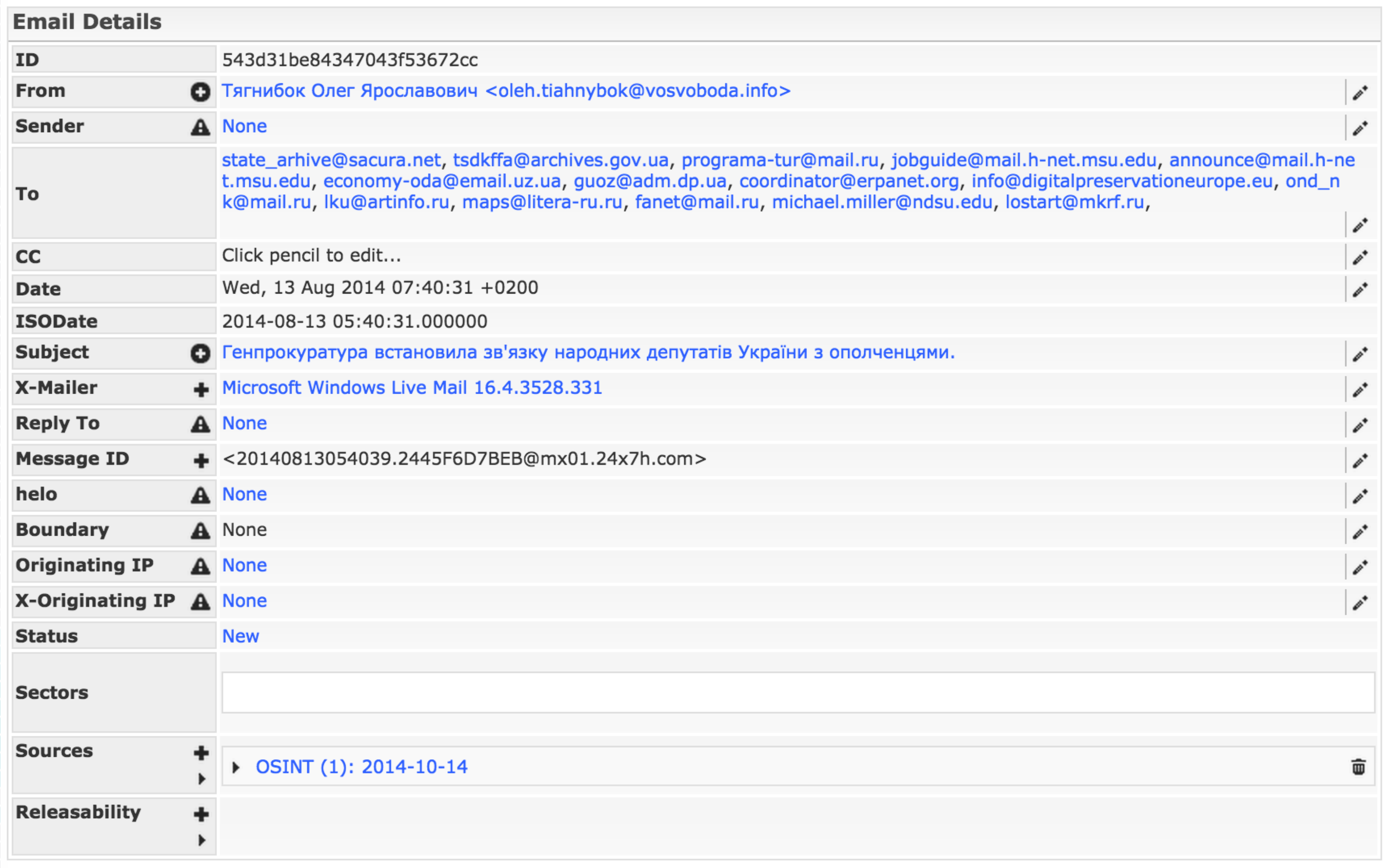
Relationships (2)

Type	Details							
	Relationship	Value	Type	Campaign	Analyst	Date	Confidence	
Indicators: 2 ▸	Related_To	2010-3	Mutex		jmilleros	2015-02-06 16:56:41	unknown	→
	Related_To	223.27.37.195	C2 URL		jmilleros	2015-02-06 16:56:41	unknown	→

Objects (2)

Type	Name	Value	Date	Analyst	Source
C2 URL: 1 ▾	C2 URL	223.27.37.195	2015-02-06	jmilleros	**Name:** Unit42 **Method:** None **Reference:** None
Mutex: 1 ▾	Mutex	2010-3	2015-02-06	jmilleros	**Name:** Unit42 **Method:** None **Reference:** None

CRITs Data Parsing



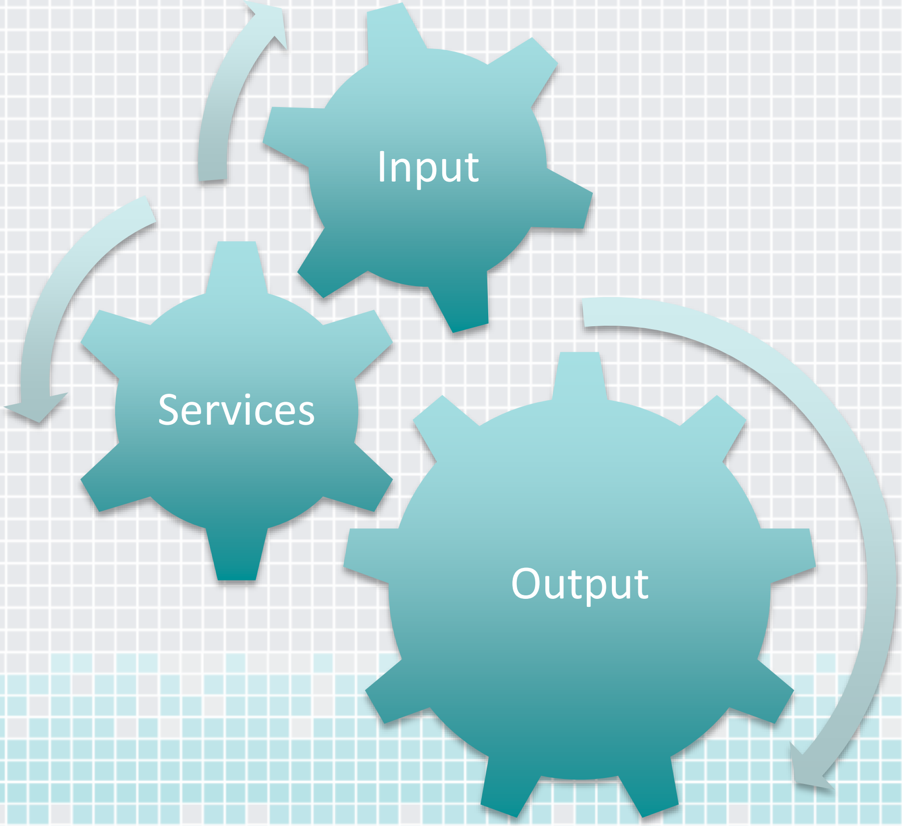
Email Details

ID	543d31be84347043f53672cc
From ⊕	Тягнибок Олег Ярославович <oleh.tiahnybok@vosvoboda.info>
Sender ⚠	None
To	state_arhive@sacura.net, tsdkffa@archives.gov.ua, programa-tur@mail.ru, jobguide@mail.h-net.msu.edu, announce@mail.h-net.msu.edu, economy-oda@email.uz.ua, guoz@adm.dp.ua, coordinator@erpanet.org, info@digitalpreservationeurope.eu, ond_nk@mail.ru, lku@artinfo.ru, maps@litera-ru.ru, fanet@mail.ru, michael.miller@ndsu.edu, lostart@mkrf.ru,
CC	Click pencil to edit...
Date	Wed, 13 Aug 2014 07:40:31 +0200
ISODate	2014-08-13 05:40:31.000000
Subject ⊕	Генпрокуратура встановила зв'язку народних депутатів України з ополченцями.
X-Mailer +	Microsoft Windows Live Mail 16.4.3528.331
Reply To ⚠	None
Message ID +	<20140813054039.2445F6D7BEB@mx01.24x7h.com>
helo ⚠	None
Boundary ⚠	None
Originating IP ⚠	None
X-Originating IP ⚠	None
Status	New
Sectors	
Sources + ▸	▸ OSINT (1): 2014-10-14
Releasability + ▸	

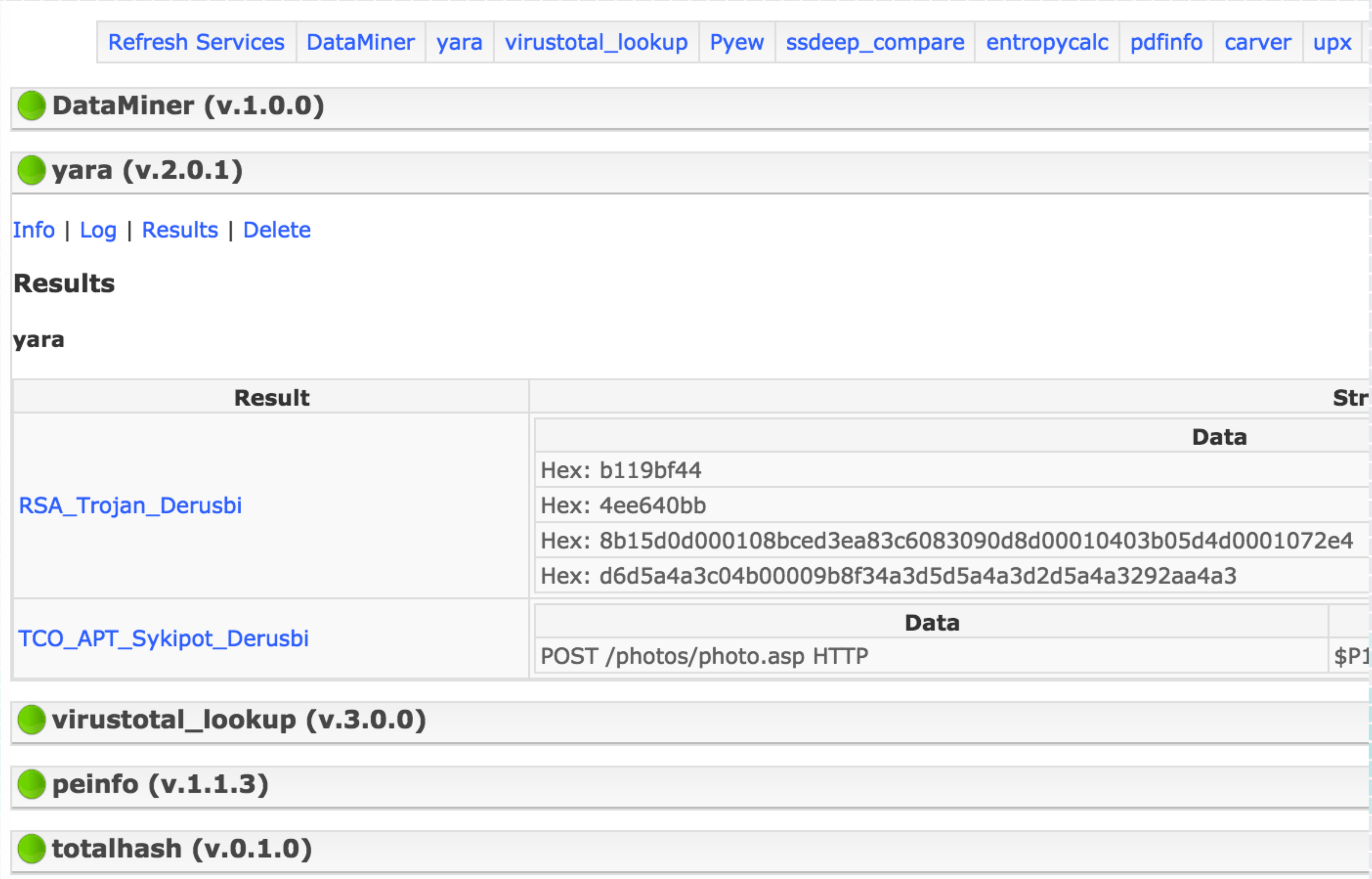
CRITS Services

Automatically process, connect and expand inputs.

- Chopshop
- Cuckoo
- OpenDNS
- PassiveTotal
- Peinfo
- SSDeep
- TAXII
- UPX
- Virustotal
- Yara
- Whois



CRITs Services



● DataMiner (v.1.0.0)

● yara (v.2.0.1)

Info | Log | Results | Delete

Results

yara

Result	Str
RSA_Trojan_Derusbi	**Data** Hex: b119bf44 Hex: 4ee640bb Hex: 8b15d0d000108bced3ea83c6083090d8d00010403b05d4d0001072e4 Hex: d6d5a4a3c04b00009b8f34a3d5d5a4a3d2d5a4a3292aa4a3
TCO_APT_Sykipot_Derusbi	**Data** POST /photos/photo.asp HTTP | $P1

● virustotal_lookup (v.3.0.0)

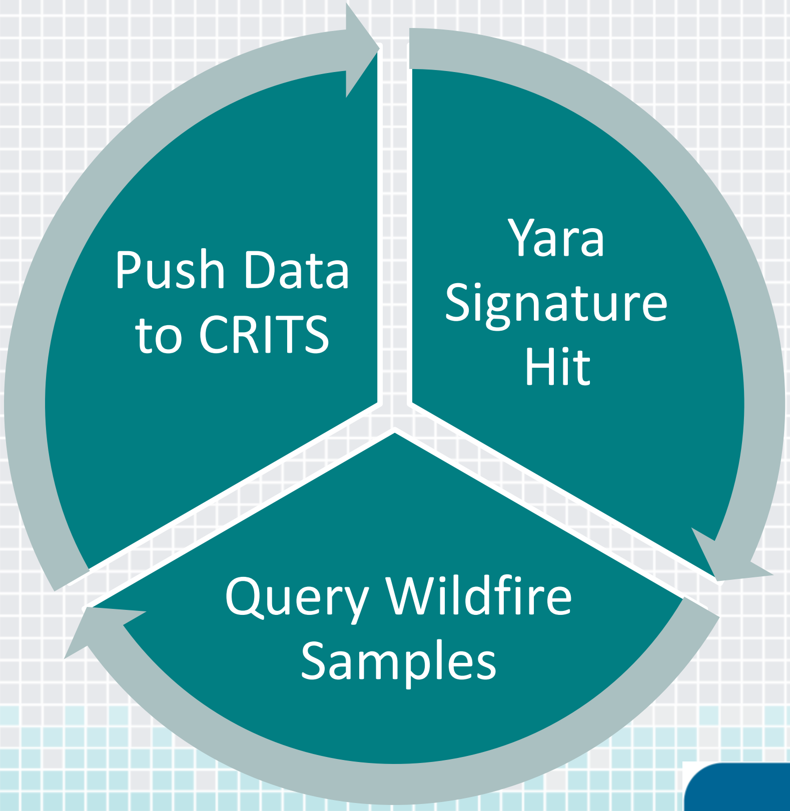
● peinfo (v.1.1.3)

● totalhash (v.0.1.0)

Best for those who “Tinker”

- Too Much Clicking…
- API allows you to automate input.
- Services allow common tasks to be built into the platform.

API Use-Case: YARA Automation



Push Data to CRITS

Yara Signature Hit

Query Wildfire Samples

Supported Structured Data Exchange Formats

TAXII

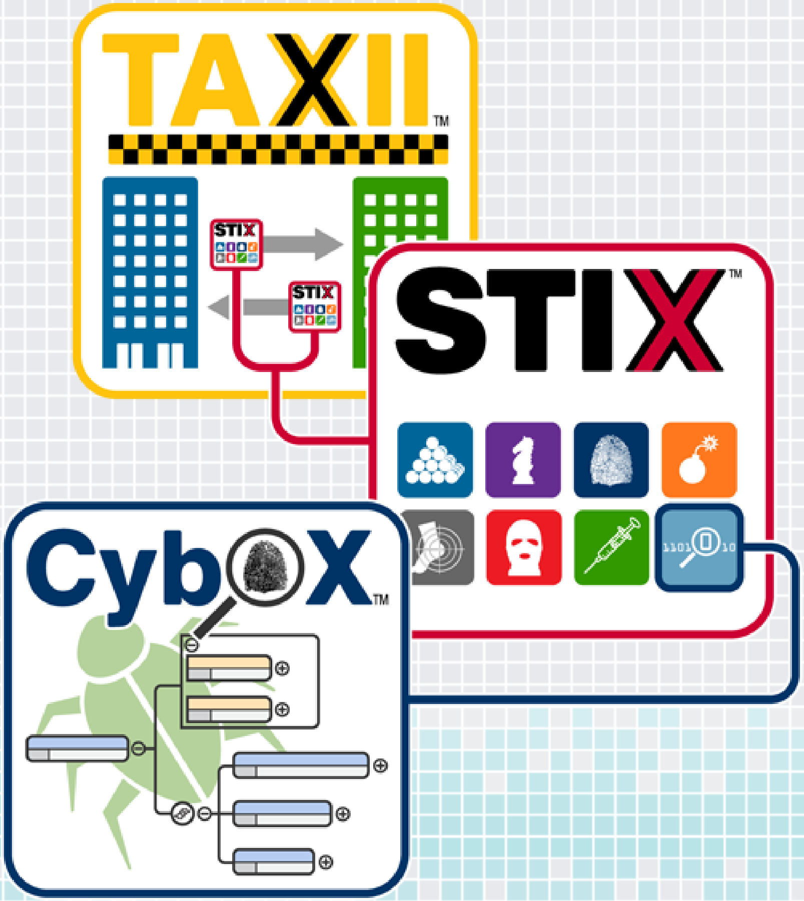
Trusted Automated Exchange of Indicator Information

STIX

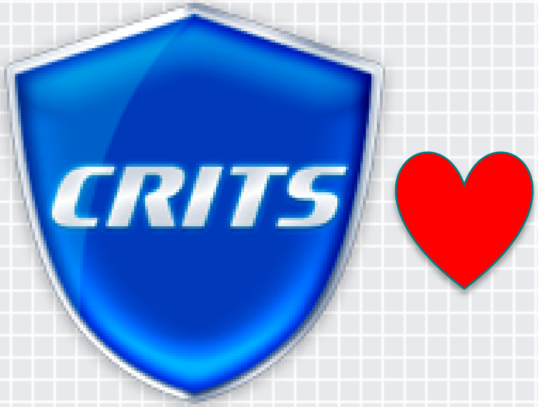
Structured Threat Information Expression

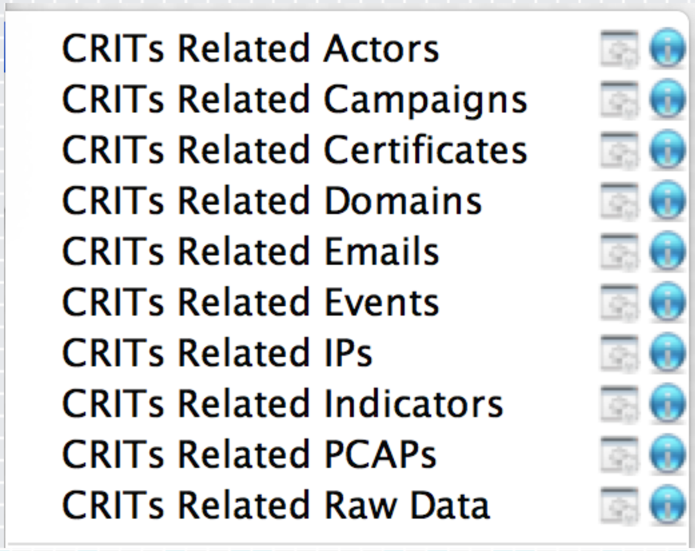
CybOX

Cyber Observable Expression



MCRITs



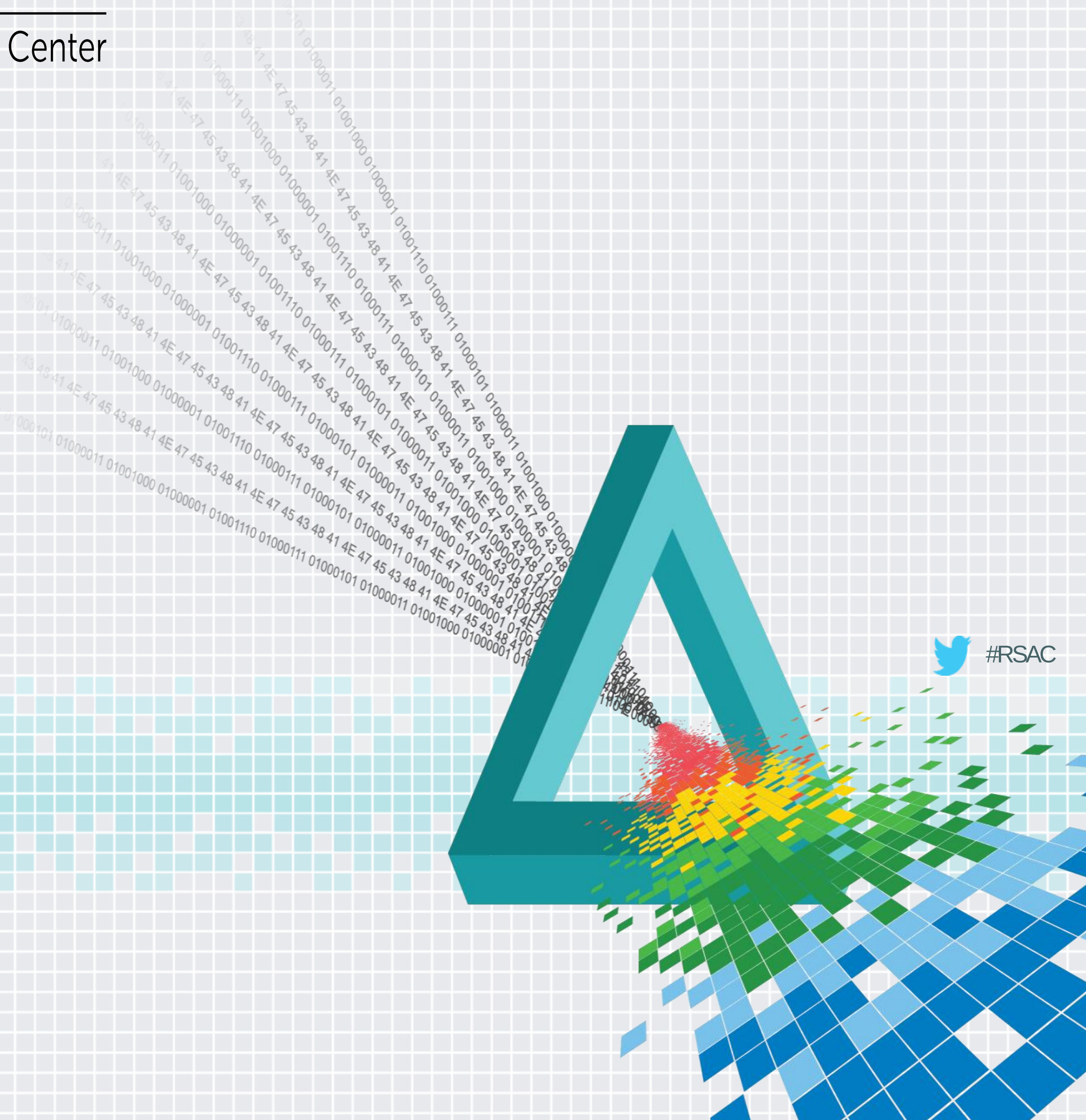

CRITs Related Actors
CRITs Related Campaigns
CRITs Related Certificates
CRITs Related Domains
CRITs Related Emails
CRITs Related Events
CRITs Related IPs
CRITs Related Indicators
CRITs Related PCAPs
CRITs Related Raw Data

Now What?

- Choose an incident and visualize it!
  - Maltego Community Edition (Try)
    - Commercial Version (Buy)
    - https://www.paterva.com/web6/products/download.php
- Get out of spreadsheets and text documents!
  - CRITs (Open Source)
    - https://github.com/crits/crits

RSA Conference2015

San Francisco | April 20-24 | Moscone Center



#RSAC

Questions