DYNAMITE ANALYTICS

Our Presenter

Jamin Becker

Chief Technology Officer
Dynamite Analytics

Jamin is a career network defender and creator of PacketTotal, the largest public PCAP analytic service in the world.

The Company

Originally founded as Vlabs in 2015

Small Business

Cybersecurity Software

Network Traffic Analysis

Network Detection and Response

Winner of multiple federal R&D awards related to Network Traffic Analysis

HQ in Atlanta Georigia

The Dynamite Family

The worlds largest public PCAP analysis platform (over 100K PCAPs)
Thousands of users worldwide

Dynamite Agent

Commercial Network Sensor for NDR
Network Metadata and Security Alerts
API Integration and Web UI

PCAP Anonymizer

Free utility for sanitizing packet-capture files
Advanced packet transformation options

DynamiteNSM

Open-source Network Security Monitor
Full stack for network traffic analysis
Native integration of Zeek and Suricata
github.com/DynamiteAI/dynamite-nsm

Briefing and Demo

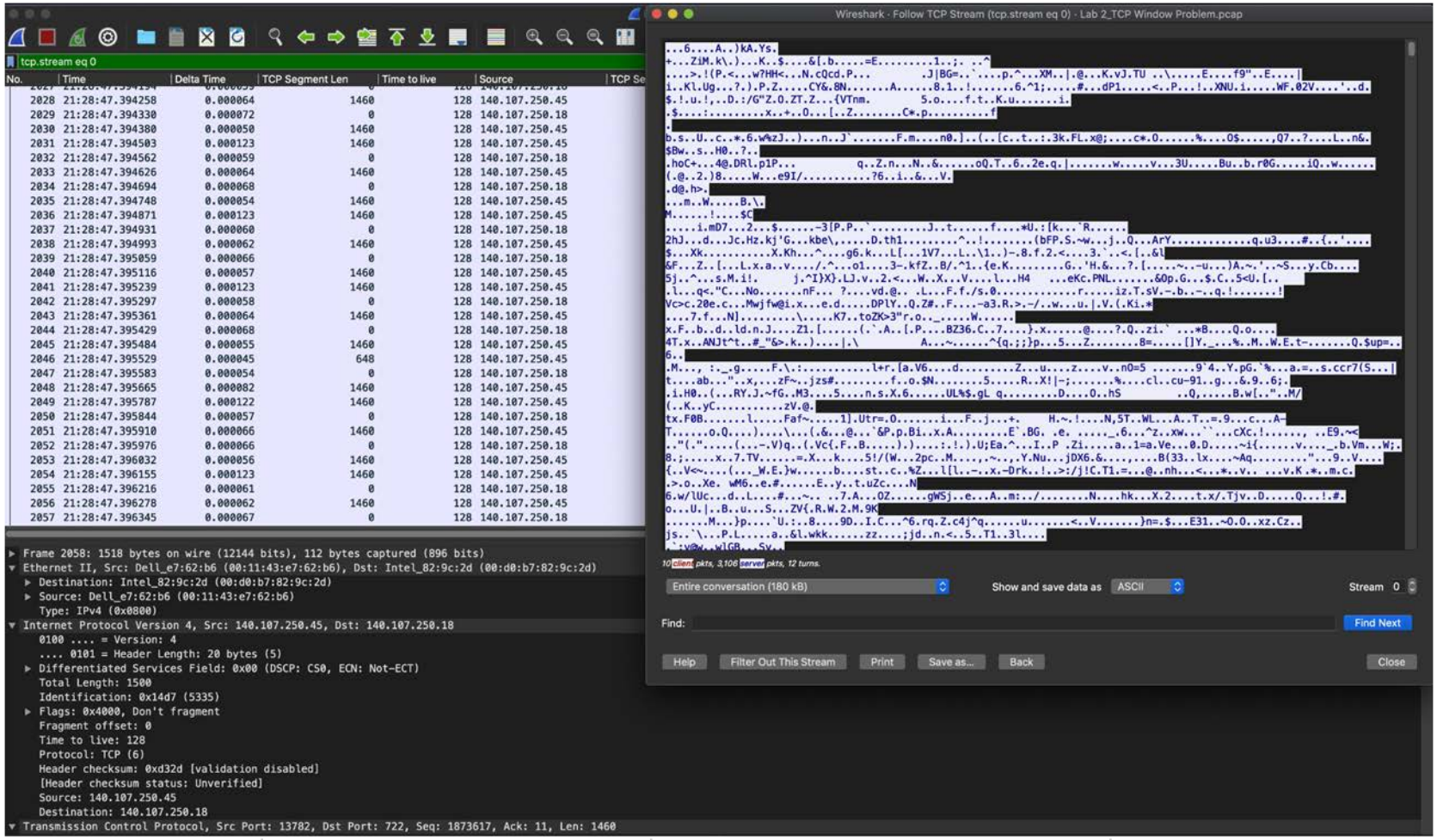
PACKETTOTAL

Design Goals

Simplify the process of PCAP analysis

Provide a platform for sharing network traffic samples

Prioritize the importance of search


tcp.stream eq 0
No. | Time | Delta Time | TCP Segment Len | Time to live | Source | TCP Se
2028 21:28:47.394258 0.000064 1460 128 140.107.250.45
2029 21:28:47.394330 0.000072 0 128 140.107.250.18
2030 21:28:47.394380 0.000050 1460 128 140.107.250.45
2031 21:28:47.394503 0.000123 1460 128 140.107.250.45
2032 21:28:47.394562 0.000059 0 128 140.107.250.18
2033 21:28:47.394626 0.000064 1460 128 140.107.250.45
2034 21:28:47.394694 0.000068 0 128 140.107.250.18
2035 21:28:47.394748 0.000054 1460 128 140.107.250.45
2036 21:28:47.394871 0.000123 1460 128 140.107.250.45
2037 21:28:47.394931 0.000060 0 128 140.107.250.18
2038 21:28:47.394993 0.000062 1460 128 140.107.250.45
2039 21:28:47.395059 0.000066 0 128 140.107.250.18
2040 21:28:47.395116 0.000057 1460 128 140.107.250.45
2041 21:28:47.395239 0.000123 1460 128 140.107.250.45
2042 21:28:47.395297 0.000058 0 128 140.107.250.18
2043 21:28:47.395361 0.000064 1460 128 140.107.250.45
2044 21:28:47.395429 0.000068 0 128 140.107.250.18
2045 21:28:47.395484 0.000055 1460 128 140.107.250.45
2046 21:28:47.395529 0.000045 648 128 140.107.250.45
2047 21:28:47.395583 0.000054 0 128 140.107.250.18
2048 21:28:47.395665 0.000082 1460 128 140.107.250.45
2049 21:28:47.395787 0.000122 1460 128 140.107.250.45
2050 21:28:47.395844 0.000057 0 128 140.107.250.18
2051 21:28:47.395910 0.000066 1460 128 140.107.250.45
2052 21:28:47.395976 0.000066 0 128 140.107.250.18
2053 21:28:47.396032 0.000056 1460 128 140.107.250.45
2054 21:28:47.396155 0.000123 1460 128 140.107.250.45
2055 21:28:47.396216 0.000061 0 128 140.107.250.18
2056 21:28:47.396278 0.000062 1460 128 140.107.250.45
2057 21:28:47.396345 0.000067 0 128 140.107.250.18
Frame 2058: 1518 bytes on wire (12144 bits), 112 bytes captured (896 bits)
Ethernet II, Src: Dell_e7:62:b6 (00:11:43:e7:62:b6), Dst: Intel_82:9c:2d (00:d0:b7:82:9c:2d)
Destination: Intel_82:9c:2d (00:d0:b7:82:9c:2d)
Source: Dell_e7:62:b6 (00:11:43:e7:62:b6)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 140.107.250.45, Dst: 140.107.250.18
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0x14d7 (5335)
Flags: 0x4000, Don't fragment
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0xd32d [validation disabled]
[Header checksum status: Unverified]
Source: 140.107.250.45
Destination: 140.107.250.18
Transmission Control Protocol, Src Port: 13782, Dst Port: 722, Seq: 1873617, Ack: 11, Len: 1460
Wireshark · Follow TCP Stream (tcp.stream eq 0) · Lab 2_TCP Window Problem.pcap
Entire conversation (180 kB)
Show and save data as
ASCII
Stream 0
Find:
Find Next
Help
Filter Out This Stream
Print
Save as...
Back
Close

Demos

- ✓ Analyzing a Packet Capture File
- ✓ Locating Captures via Search
- ✓ Locating Captures via Similar Search

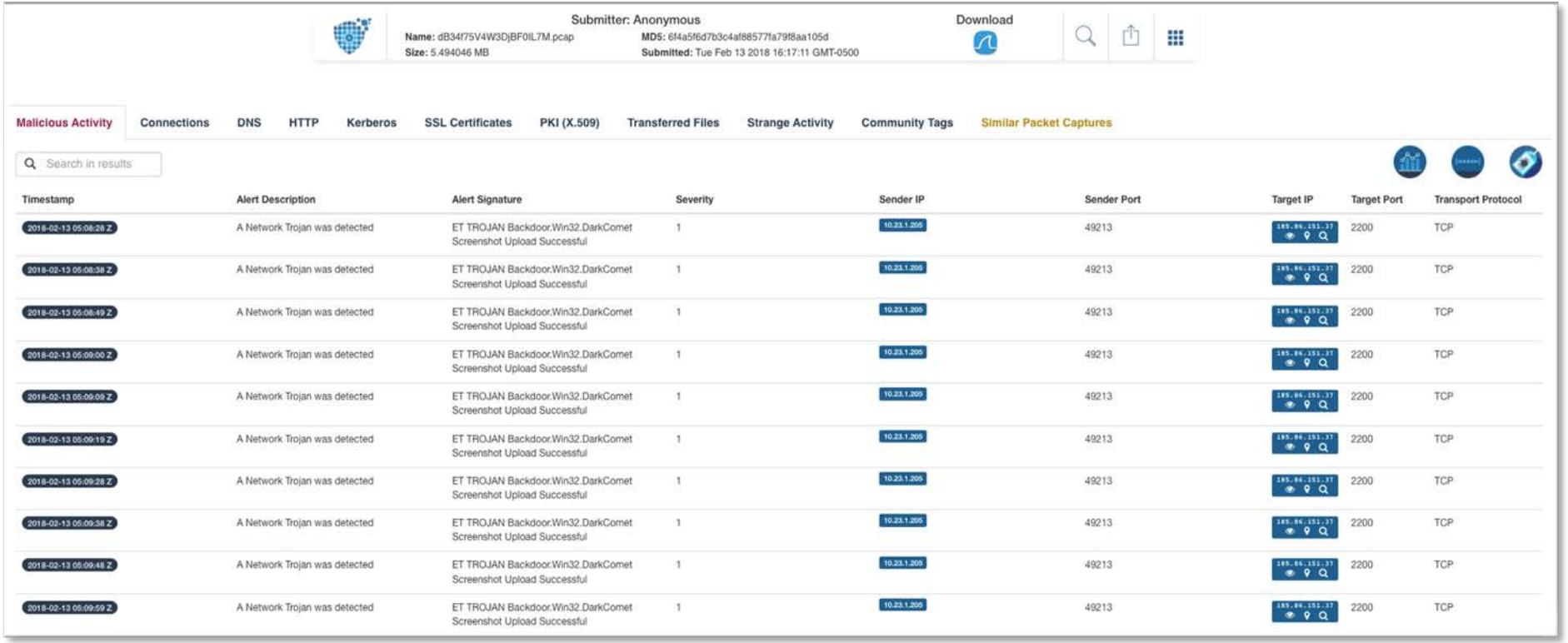
Be careful what you upload!

- ✓ Avoid uploading pcaps of home or work networks
- ✓ Avoid capturing traffic containing information about your environment
- ✓ Consider using capture filters, only capture the traffic you wish to analyze/share
- ✓ Consider capturing pcaps from sandboxed environment

Analyzing a Packet Capture File

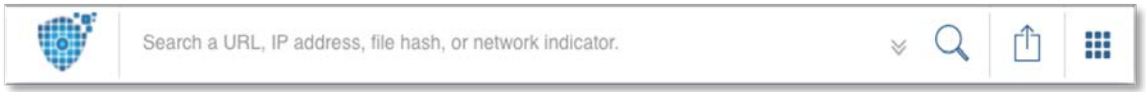
- ✓ PacketTotal supports both pcap and pcapng file-types
- ✓ You can upload from any page on the site
- ✓ Once uploaded your PCAP will be queued for analysis
- ✓ Time to analyze varies

Console View



Locating Captures via Search

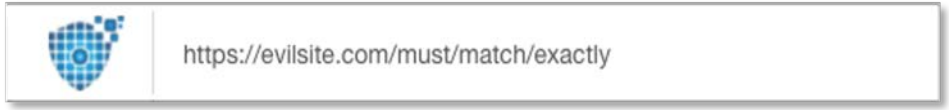
- ✓ Navigate to packettotal.com/app/search/ to get started
- ✓ Supported Query Types:
  - Free Text
  - Field/Value
  - Boolean



Free Text Queries

IP Addresses

URLs



Domain Wildcards

Field/Value Queries

IP Fields

Metadata Fields

Protocol Fields

Boolean Queries

OR

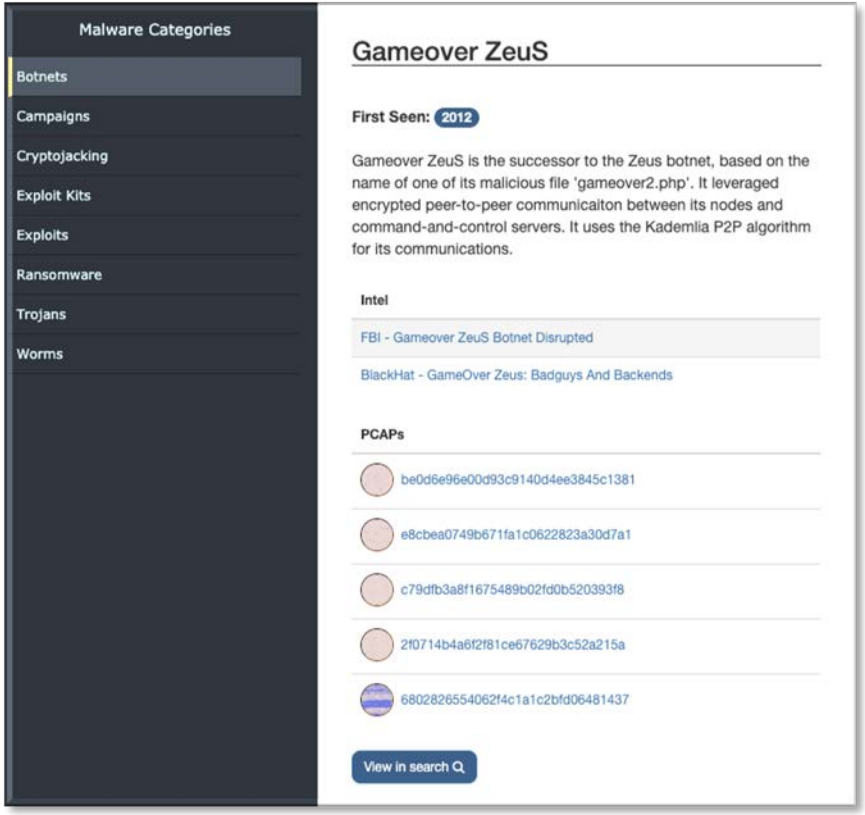
AND

Grouping

Malware Repository

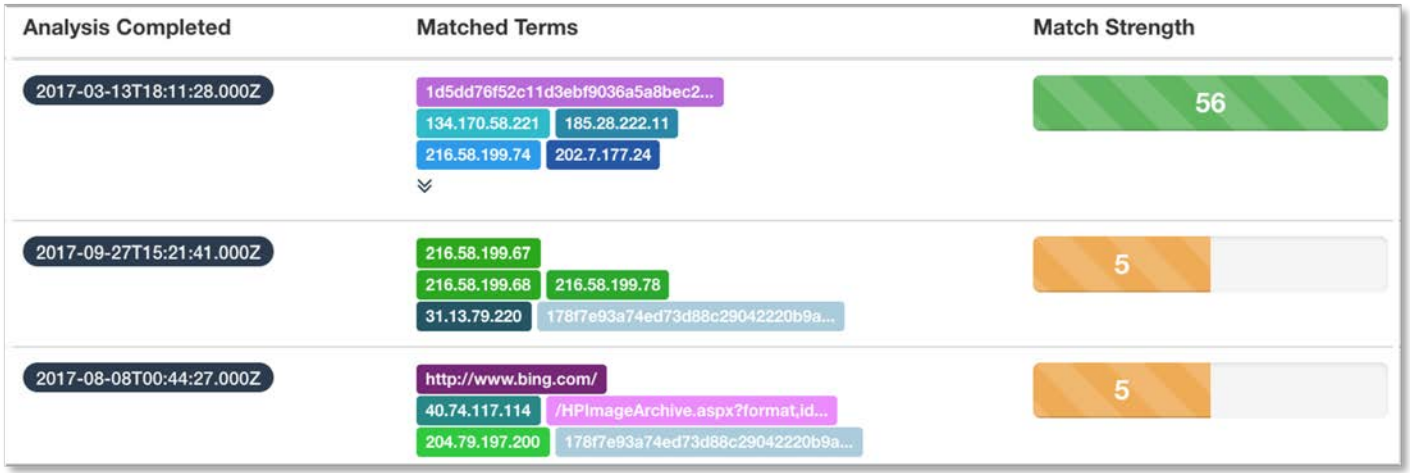
- ✓ Maintained by Dynamite
- ✓ Locate common strains of malware
- ✓ Search related network indicators

packettotal.com/malware-archive.html



Locating Captures via Similar Search

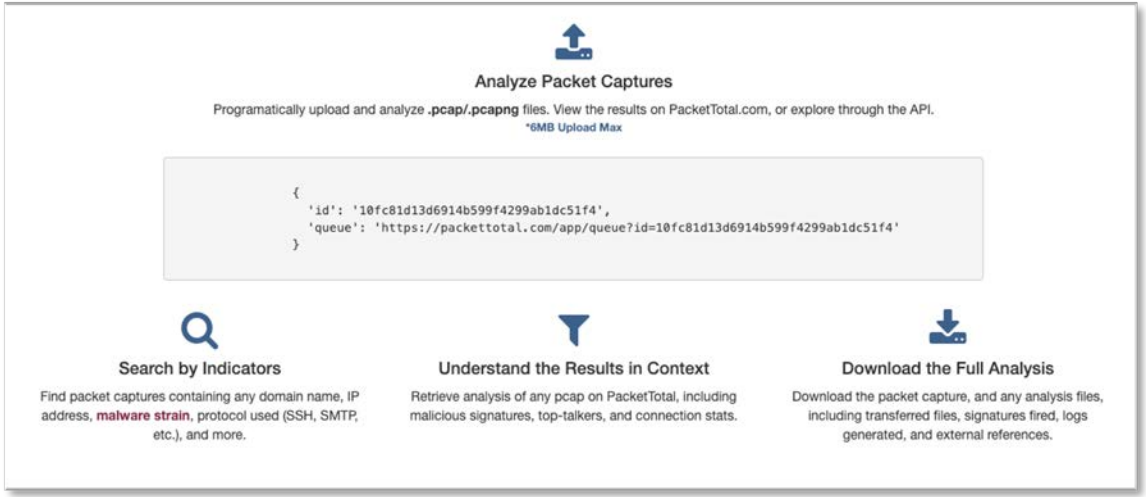
- ✓ Can be thought of as a “reverse image search”
- ✓ "similar" pcaps have indicators in common
  - domain name, an IP, a file
- ✓ Go to “Similar PCAPs” tab **Similar Packet Captures**



Yes, There is an API!

- ✓ Search API is available to beta testers
- ✓ Automation with programmatic search
- ✓ Many other API-only features
- ✓ Request an API key at

packettotal.com/api.html

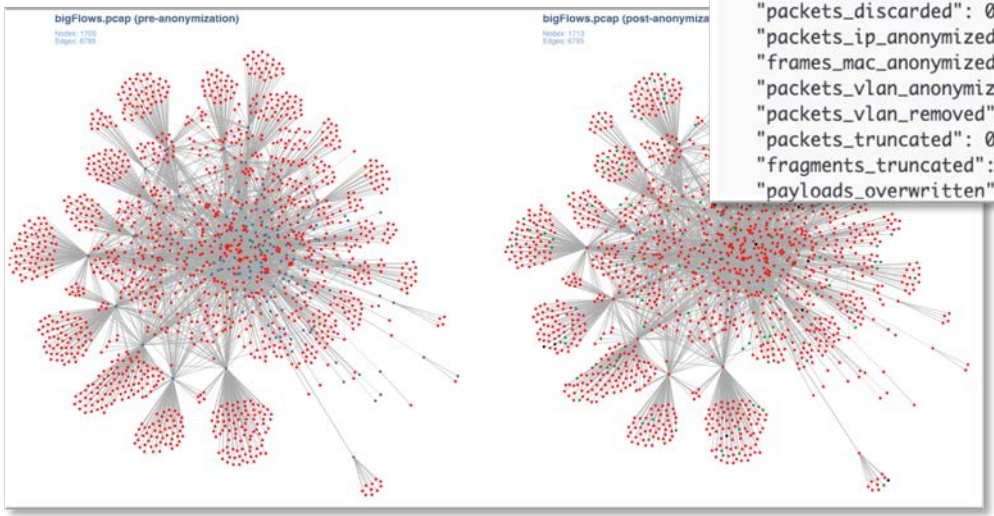


APPENDIX

PCAP Anonymizer

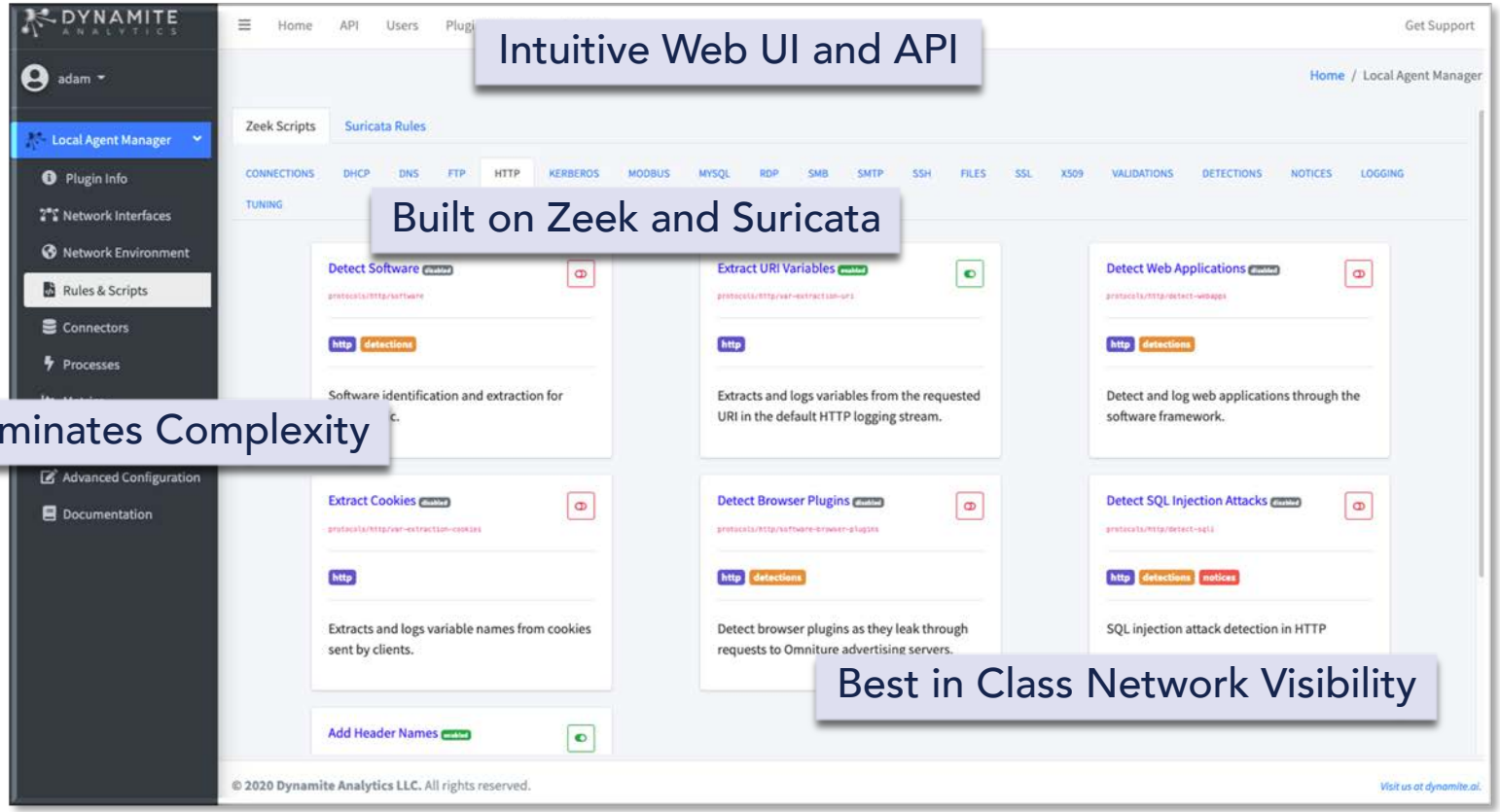
- Highly Customizable via CLI or Options File
- Anonymize IP and MAC addresses
- Anonymize ARP, ICMP, VLAN

```
adam@mbp2 cmd % ./anonymizer -source ~/pcaps/bigFlows.pcap -ip full -mac full -store-mappings -graph
{
    "source_file": "bigFlows.pcap",
    "output_file": "/tmp/bigFlows.pcap-anonymized",
    "graph_file": "/tmp/bigFlows.pcap-anonymized-graph.html",
    "ip_mapping_file": "/tmp/bigFlows.pcap-anonymized.ips",
    "mac_mapping_file": "/tmp/bigFlows.pcap-anonymized.macs",
    "packets_read": 791615,
    "packets_analyzed": 791615,
    "packets_written": 791581,
    "packets_discarded": 0,
    "packets_ip_anonymized": 787315,
    "frames_mac_anonymized": 787315,
    "packets_vlan_anonymized": 0,
    "packets_vlan_removed": 0,
    "packets_truncated": 0,
    "fragments_truncated": 0,
    "payloads_overwritten": 0,
```



- Truncate and mask payloads
- Generate interactive graphs for visual analysis
- Packet filtering, CIDR support and more

Dynamite Agent



Intuitive Web UI and API

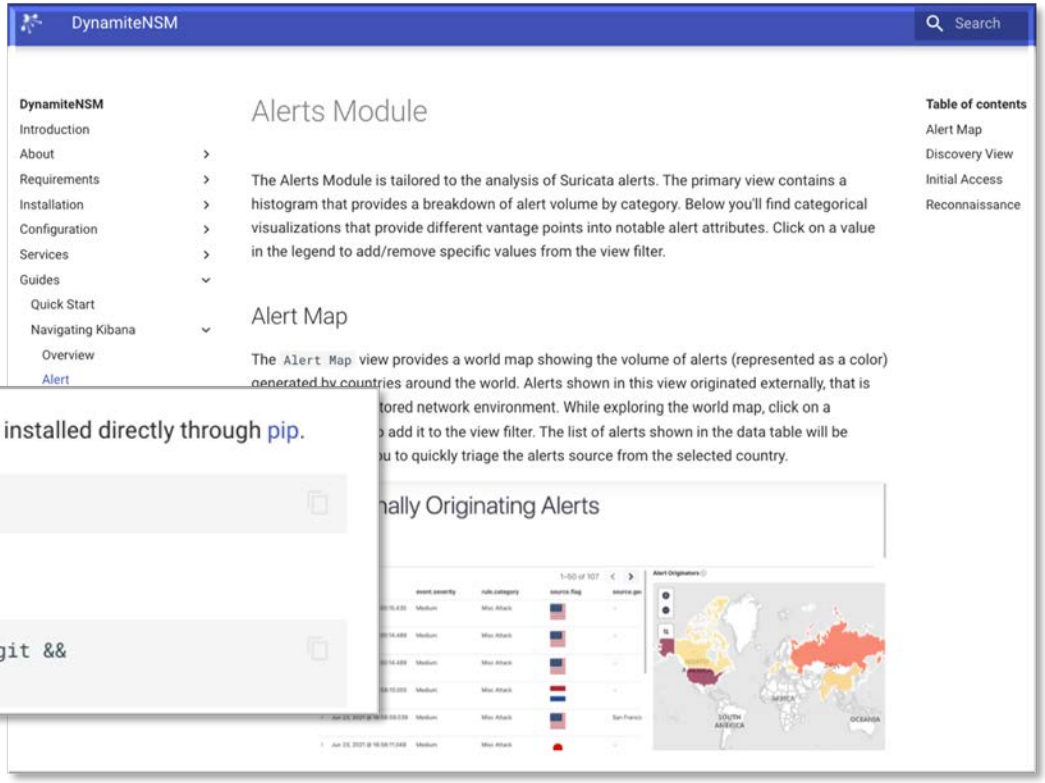
Built on Zeek and Suricata

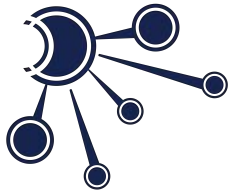
Eliminates Complexity

Best in Class Network Visibility

DynamiteNSM

- Open-source Network Security Monitor
- Full Network Monitoring Stack + SDK
- Simple Zeek and Suricata Management
- Full Data Ingest Pipeline
- Many Analysis and Hunting Dashboards





DYNAMITE
ANALYTICS

Thank You!

Jamin Becker

info@dynamite.ai

dynamite.ai
github.com/DynamiteAI

Check out Free Dynamite Agent Starter on AWS Marketplace

"Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Networking and Information Technology Research and Development Program."

The Networking and Information Technology Research and Development (NITRD) Program

Mailing Address: NCO/NITRD, 2415 Eisenhower Avenue, Alexandria, VA 22314

Physical Address: 490 L'Enfant Plaza SW, Suite 8001, Washington, DC 20024, USA Tel: 202-459-9674, Fax: 202-459-9673, Email: nco@nitrd.gov, Website: https://www.nitrd.gov