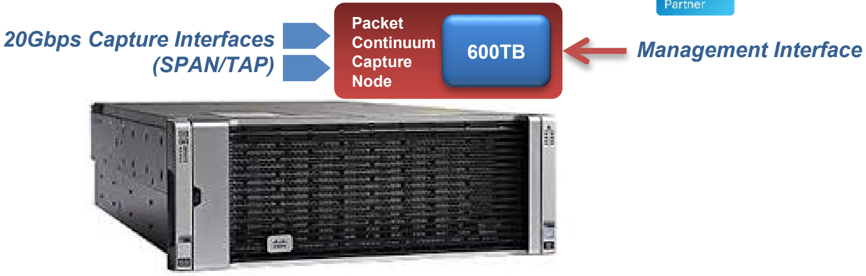
Packet Continuum UCS – Product Offering

Type	Capture Rate Capacity	Timeline Capacity	Federation Capacity	Target Platform	Available as	
Lite	up to 2Gbps	• 40TB = 3^{++} Days@1Gbps • 200TB Max (1+4 cluster)	up to 10,000 capture points	1U Cisco UCS C220 M5 Rack LFF Server	Software license	Integrated Appliance
CSPA Upgrade	4^{++}Gbps	• 40TB = 3^{++} Days @1Gbps • No Cluster Expansion		2U Cisco Security Packet Analyzer	Software license	
Deployable	up to 10Gbps	• Up to 100TB • 500TB Max (1+4 cluster)		NextServer-X Portable*		Integrated Appliance
Enterprise	up to 10Gbps	• 100TB = 1^{++} Days@10Gbps • 500TB Max (1+4 cluster)		2U Cisco UCS C240 M5 Rack LFF Server	Software license	Integrated Appliance
Extreme	up to 20Gbps	• 600TB = 6^{++} Days@10Gbps • 5.4PB Max (1+8 cluster)		4U Cisco UCS S3260 Storage Server	Software license	
Federated Group	Unlimited	• Unlimited		Multiple UCS servers	Software license	

* NOTE: NextComputing's NextServer-X Portable/Deployable is a TSA-compliant carry-on (<35lbs) and also suitable for mobile deployment of virtualized Stealthwatch modules, with or without Packet Continuum software.

Extreme Capture Node



20Gbps Capture Interfaces (SPAN/TAP)

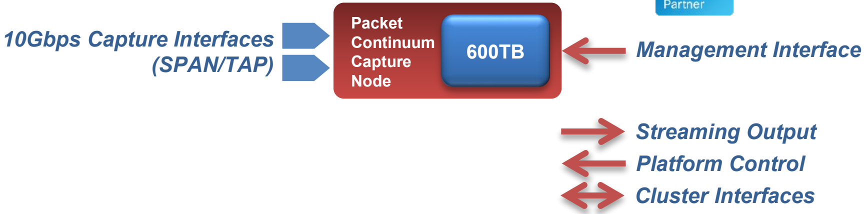
Packet Continuum Capture Node

600TB

Management Interface

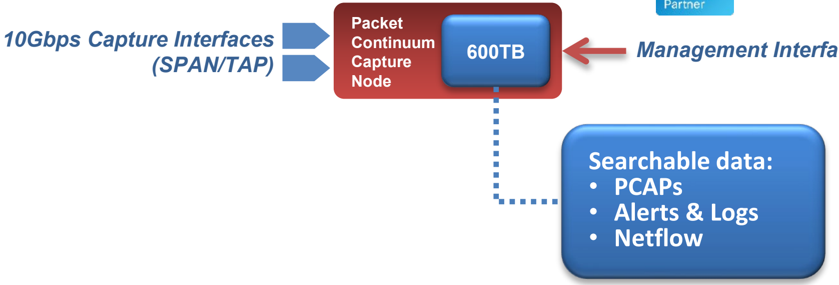
Specification	Description
Capture Rate	• **20Gbps** sustained PEAK capture rate, via 2x10G (or 4x1G) capture interfaces (SFP+ SR and/or RJ-45) • Zero packet loss (deterministic), even with full packet analytics (eg. 50,000 active Snort/Suricata alerts) • Very fast PCAP search, simultaneous with capture operations
Capture Timeline	• **600TB** Capture Store – dedicated to ***actively-searchable*** PCAP data • Capture Timeline, based on data compression ratio which is network dependent: ○ **3^{++} Days @ 20Gbps** AVERAGE capture rate ○ **6^{++} Days @ 10Gbps** AVERAGE capture rate ○ **8^{++} Weeks @ 1Gbps** AVERAGE capture rate
Expansion	• Unlimited Capture Timeline, by adding **up to 4 Cluster Nodes**, or federating multiple Capture Nodes • Unlimited Capture Rate, by aggregating federated Capture Nodes
Hardware Platform	• **4U x 27" standard-SKU rackmount: Cisco UCS S3260 Storage Server** • No proprietary hardware.
Software Platform	• CentOS, or Red Hat EL. No modifications to OS or drivers. • Role-Based Access Control via SSO, LDAP, RADIUS, etc

Interfaces



Specification	Description
Management Interface	• For remote access by the Web-based User Interface • For programmatic access via the REST/API
Stream Search Output Interface	• For streaming replay of PCAP search results. For example, for analysis by legacy tools. • For Alert/Event Log Forwarding. For example, selective log/metadata streaming to 3rd party systems. • For “Active Defense” messaging. For example, when Threat IP activity is detected.
IPMI Platform Control Interface	• For device control during "lights out" operation, server monitoring, remote re-boot, etc
Cluster Node Interfaces	• For point-to-point fiber connection for multiple Cluster Nodes for additional storage expansion that is actively-searchable

Real-Time Packet Analytics



10Gbps Capture Interfaces (SPAN/TAP)

Packet Continuum Capture Node

600TB

Management Interface

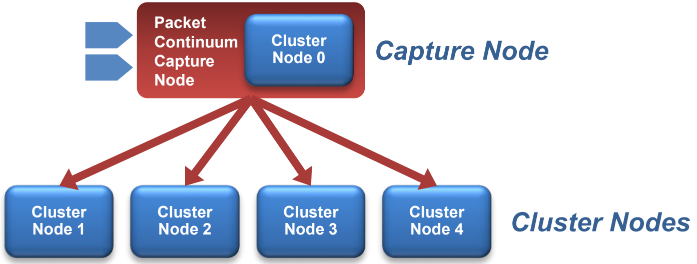
Searchable data:

- PCAPs
- Alerts & Logs
- Netflow

Specification	Description
IDS Alerting	• Up to 50,000 active Snort/Suricata IDS rules, simultaneous with PCAP capture/search • Up to 1M Suspicious ThreatIP alerts • Defended Assets & Defended Services • User-defined, or select for pre-packaged libraries
IoC Alerting & Augmentation	• BPF-based Active Triggers • Suspicious Domains & IP Addresses • Suspicious Files (eg. MD5 Hashes) • Suspicious SSL/TLS activity (eg. JA3 Signatures) • User-defined, or select from pre-packaged libraries
DPI Event Logging	• File Detection, Emails, DNS, SMB, SSL/TLS, VOIP, User-Agent – and NetFlow V9 generation
Retrospective Detection	• “SigDetect” feature to search-back over the entire timeline for emerging 0-Day threats, using Snort/Suricata rulesets and other Indicators of Compromise (IoC)

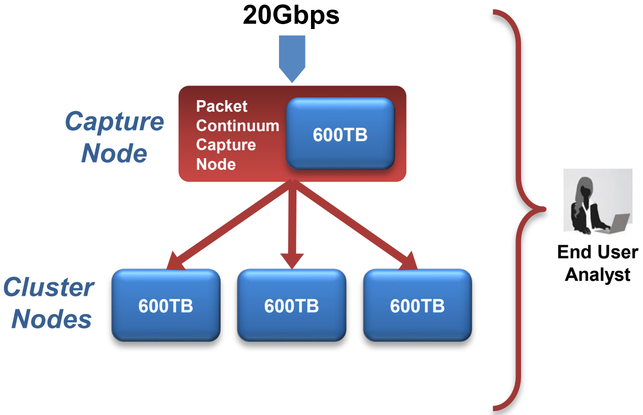
Capture Clusters

“1+4 Capture Cluster”

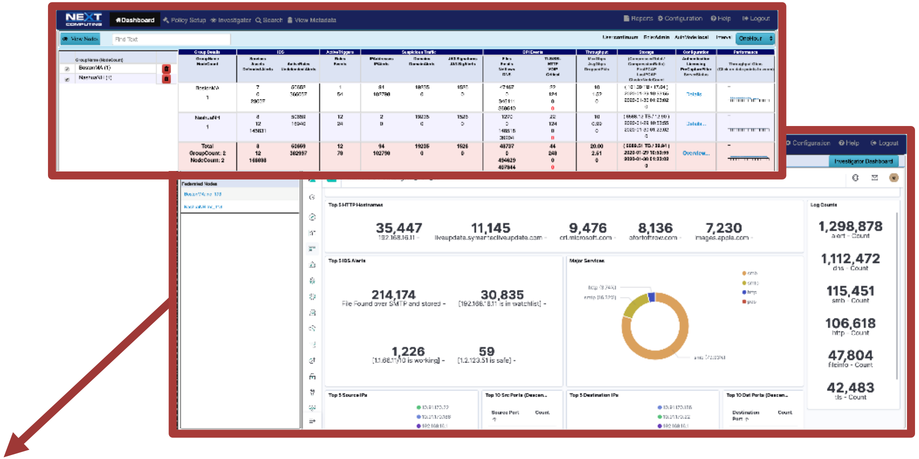


Specification	Description
Capture Timeline	• Each Cluster Node provides ***actively-searchable*** storage expansion matching Capture Node storage ○ ***Note: PCAP search times remain constant***, as Capture Store increases • For example, a “1+4 Capture Cluster” has a Capture Timeline of 5x vs a standalone Capture Node
Expansion Options	• The number of Cluster Nodes per individual Capture Node is limited (up to 4 or 8) • Unlimited timeline expansion is possible by “Federating” multiple Capture Clusters
Hardware Platform	• Cluster Nodes deploy on the same underlying server platform as the matching Capture Node • Capture Store capacity must be the same for all Capture/Cluster Nodes in the same cluster
Software Platform	• CentOS, or Red Hat EL

Capture Clusters

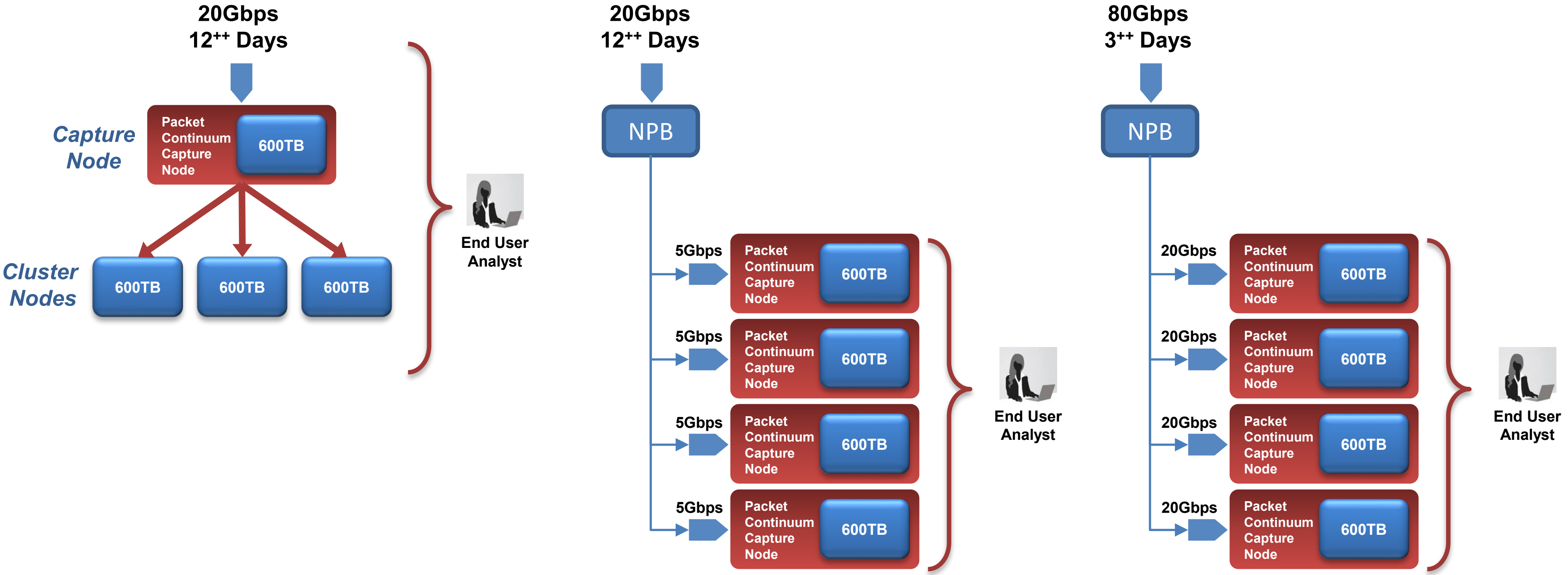


"Federated"
WebGUI & REST/API



Simplified Analyst Workflows:
(1) PIVOT to Federated PCAP Search
(2) INVESTIGATE with remote views & iterative search
(3) REPORT and/or extract PCAPs into 3rd party tools.

Federate to Scale Timeline or Capture Rate



20Gbps
12⁺⁺ Days

Capture Node

Packet Continuum Capture Node

600TB

Cluster Nodes

600TB

600TB

600TB

End User Analyst

20Gbps
12⁺⁺ Days

NPB

5Gbps – Packet Continuum Capture Node – 600TB

5Gbps – Packet Continuum Capture Node – 600TB

5Gbps – Packet Continuum Capture Node – 600TB

5Gbps – Packet Continuum Capture Node – 600TB

End User Analyst

80Gbps
3⁺⁺ Days

NPB

20Gbps – Packet Continuum Capture Node – 600TB

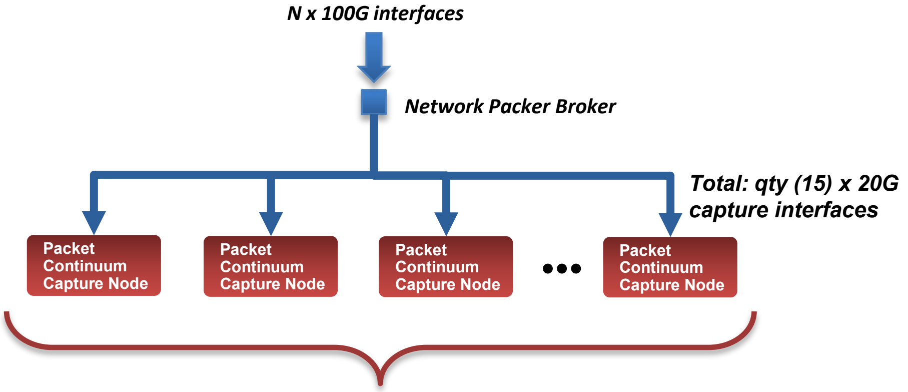
20Gbps – Packet Continuum Capture Node – 600TB

20Gbps – Packet Continuum Capture Node – 600TB

20Gbps – Packet Continuum Capture Node – 600TB

End User Analyst

Telco Example: 300Gbps for 6 Days required at a PoP Site


N x 100G interfaces
Network Packer Broker
Total: qty (15) x 20G capture interfaces
Packet Continuum Capture Node
Packet Continuum Capture Node
Packet Continuum Capture Node
•••
Packet Continuum Capture Node

Capture Rate:

- ***300Gbps PEAK** continuous lossless capture*
- *IDS alerting at line rate*
- *Simultaneous PCAP search*
- *qty 15 Standalone Capture Nodes*

qty 15	*Standalone Capture Nodes*
x 20 Gbps	*Average capture rate for 2 Days Timeline*
300 Gbps	*Total aggregate capture rate*

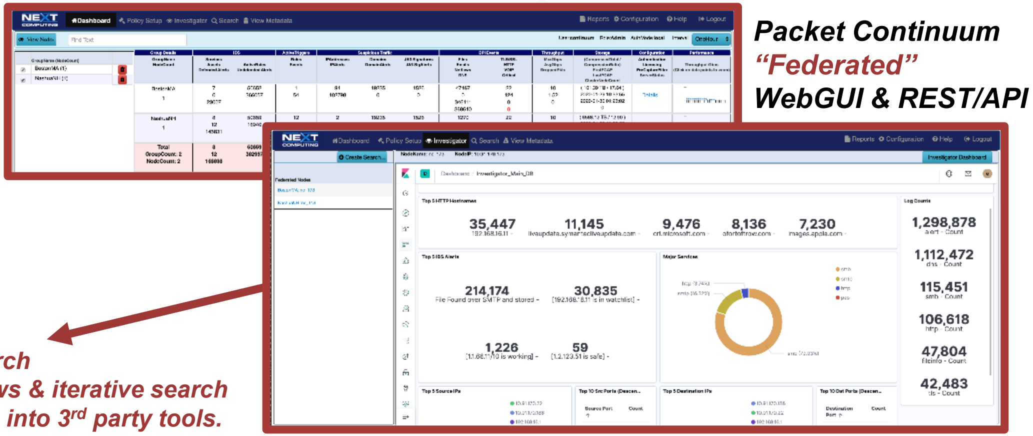
Capture Timeline:

- ***6 Days**, assuming 300Gbps AVERAGE rate, 2:1 data compression*
- *9.0PB Total Capture Store*

Rackspace:

- *qty 15 x 4U servers:*
  4U Cisco UCS S3260 Storage Server, with
  Up to 20Gbps lossless Capture Rate
  600TB Capture Store

End User Analyst



Packet Continuum "Federated" WebGUI & REST/API

Simplified Analyst Workflows:
(1) PIVOT to Federated PCAP Search
(2) INVESTIGATE with remote views & iterative search
(3) REPORT and/or extract PCAPs into 3rd party tools.

Telco Example: 59 Federated PoP Sites

System-wide Capture Rate:

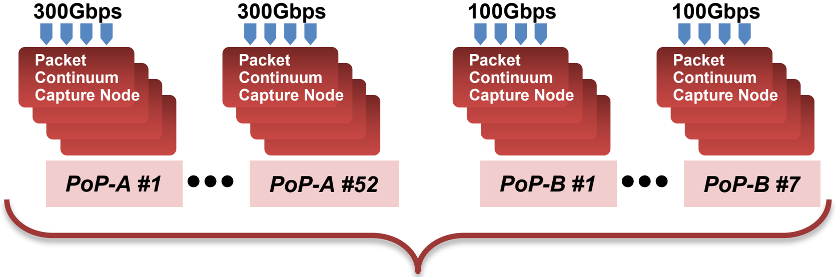
52 PoP-A sites (300Gbps each)
+ 7 PoP-B sites (100Gbps each)
16.3 Tbps continuous lossless capture (aggregate)

System-wide Capture Timeline:

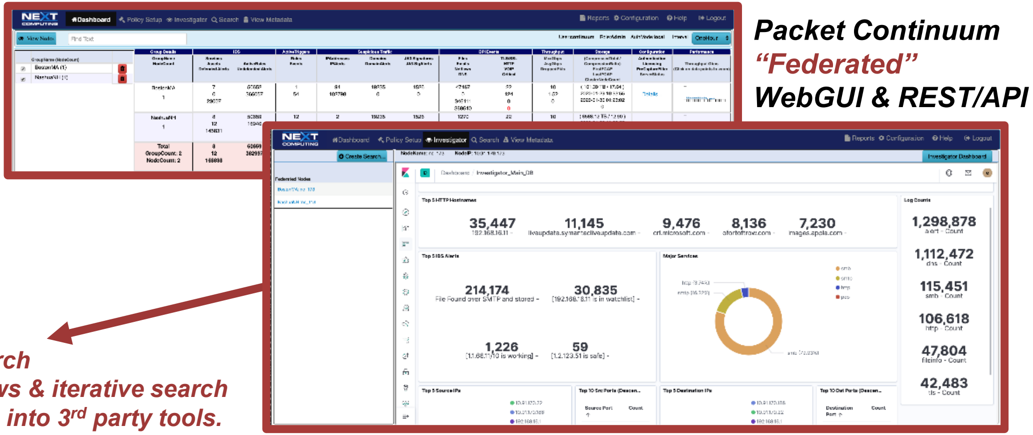
52 PoP-A sites (9.0PB each, for 6 Day timeline)
+ 7 PoP-B sites (7.5PB each, for 2 Weeks timeline)
520PB Capture Store

Rackspace:

52 PoP-A sites (15 x 4U servers each)
+ 7 PoP-B sites (12 x 4U servers each)
864 total # of 4U servers


300Gbps
Packet Continuum Capture Node
PoP-A #1
●●●
300Gbps
Packet Continuum Capture Node
PoP-A #52
100Gbps
Packet Continuum Capture Node
PoP-B #1
●●●
100Gbps
Packet Continuum Capture Node
PoP-B #7

End User Analyst



Top 5 HTTP Hostnames

35,447 192.168.16.11
11,145 liveupdate.symantecliveupdate.com
9,476 crl.microsoft.com
8,136 ctldl.windowsupdate.com
7,230 images.apple.com

Top 5 IDS Alerts

214,174 File Found over SMTP and stored
30,835 [192.168.18.11 is in watchlist]
1,226 [1.1.68.11/10 is working]
59 [1.2.123.51 is safe]

Major Services

Log Counts

1,298,878 alert - Count
1,112,472 dns - Count
115,451 smb - Count
106,618 http - Count
47,804 fileinfo - Count
42,483 tls - Count

Top 5 Source IPs

Top 10 Src Ports (Descen...

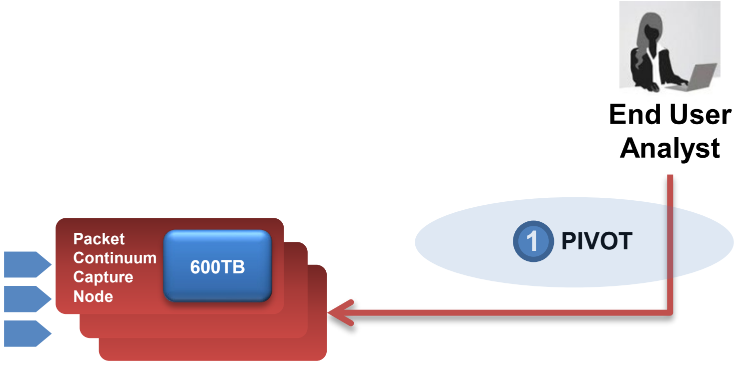
Top 5 Destination IPs

Top 10 Dst Ports (Descen...

Packet Continuum "Federated" WebGUI & REST/API

Simplified Analyst Workflows:
(1) PIVOT to Federated PCAP Search
(2) INVESTIGATE with remote views & iterative search
(3) REPORT and/or extract PCAPs into 3rd party tools.

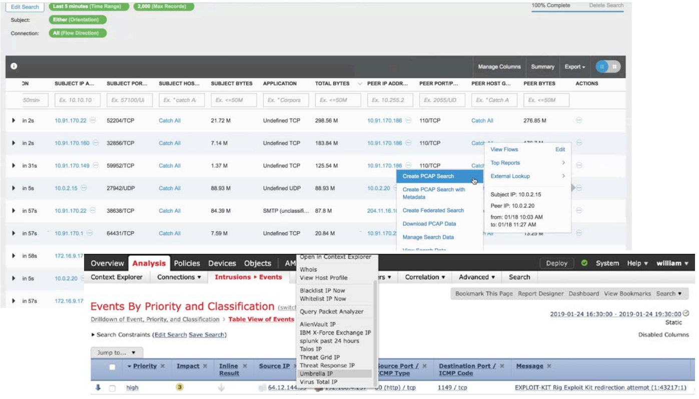
First, Pivot from Cisco Security



Pivot-to-PCAP from:

- **Cisco Stealthwatch Console**
- **Cisco Firepower Mgmt Center**
- **Or any event from Cisco, or 3rd parties**

Federated Group, or a Standalone Capture Node



Subject: Either (Orientation)

Connection: All (Flow Direction)

ON	SUBJECT IP A...	SUBJECT POR...	SUBJECT HOS...	SUBJECT BYTES	APPLICATION	TOTAL BYTES	PEER IP ADDR...	PEER PORT/P...	PEER HOST G...	PEER BYTES	ACTIONS
50min	Ex. 10.10.10	Ex. 57100/U	Ex. "catch A	Ex. <=50M	Ex. "Corpora	Ex. <=50M	Ex. 10.255.2	Ex. 2055/UD	Ex. "Catch A	Ex. <=50M	
in 2s	10.91.170.22	52204/TCP	Catch All	21.72 M	Undefined TCP	298.56 M	10.91.170.186	110/TCP	Catch All	276.85 M	
in 2s	10.91.170.160	32856/TCP	Catch All	7.14 M	Undefined TCP	183.84 M	10.91.170.186	110/TCP	Catc		
in 31s	10.91.170.149	59952/TCP	Catch All	1.37 M	Undefined TCP	125.54 M	10.91.170.186	110/TCP	Catc		
in 5s	10.0.2.15	27942/UDP	Catch All	88.93 M	Undefined UDP	88.93 M	10.0.2.20				
in 57s	10.91.170.22	38638/TCP	Catch All	84.39 M	SMTP (unclassifi...	87.8 M	204.11.16.1				
in 57s	10.91.170.1	64431/TCP	Catch All	7.59 M	Undefined TCP	20.84 M	10.91.170.2			13.25 M	
in 58s	172.16.9.17										
in 5s	10.0.2.20										
in 57s	172.16.9.17										

Subject IP: 10.0.2.15
Peer IP: 10.0.2.20
from: 01/18 10:03 AM
to: 01/18 11:27 AM

Events By Priority and Classification (switch

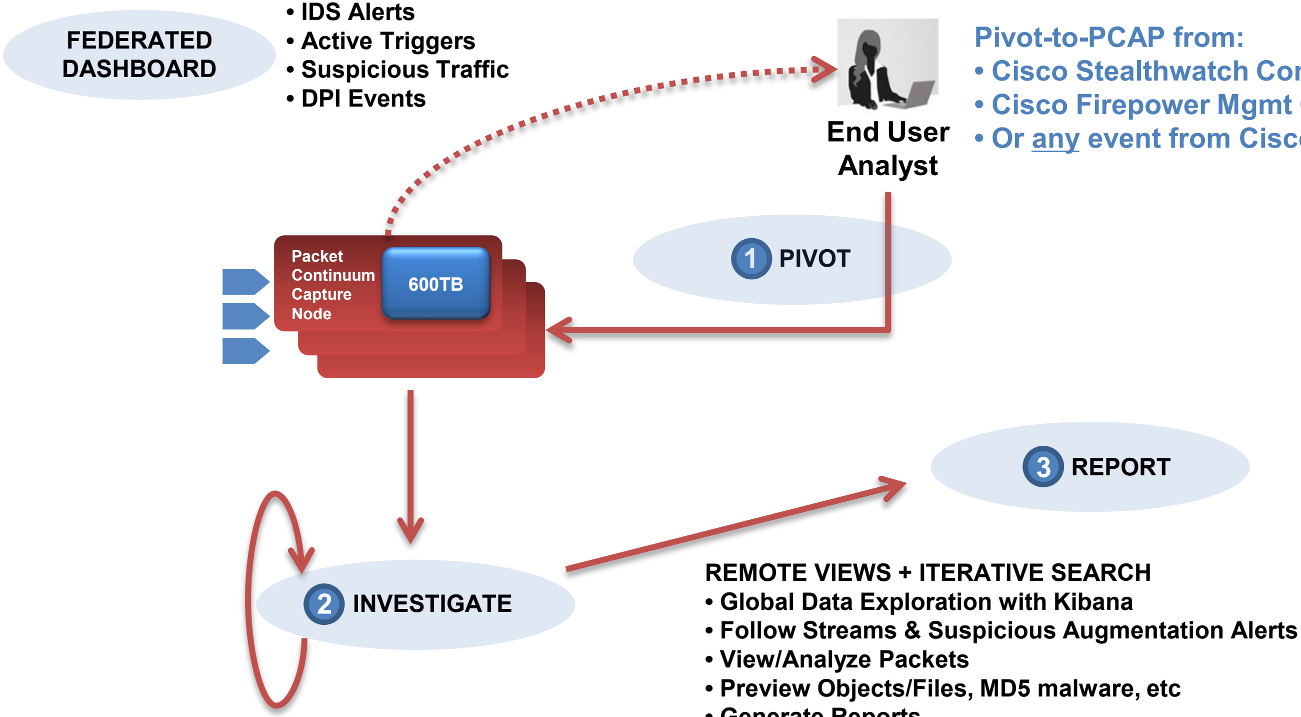
Drilldown of Event, Priority, and Classification › Table View of Events

▸ Search Constraints (Edit Search Save Search)

2019-01-24 16:30:00 - 2019-01-24 19:30:00
Static

	Priority	Impact	Inline Result	Source IP		Source Port / ICMP Type	Destination Port / ICMP Code	Message
□	high	3		64.12.144.		80 (http) / tcp	1149 / tcp	EXPLOIT-KIT Rig Exploit Kit redirection attempt (1:43217:1)

Simplified PCAP Workflow: Summary



- IDS Alerts
- Active Triggers
- Suspicious Traffic
- DPI Events

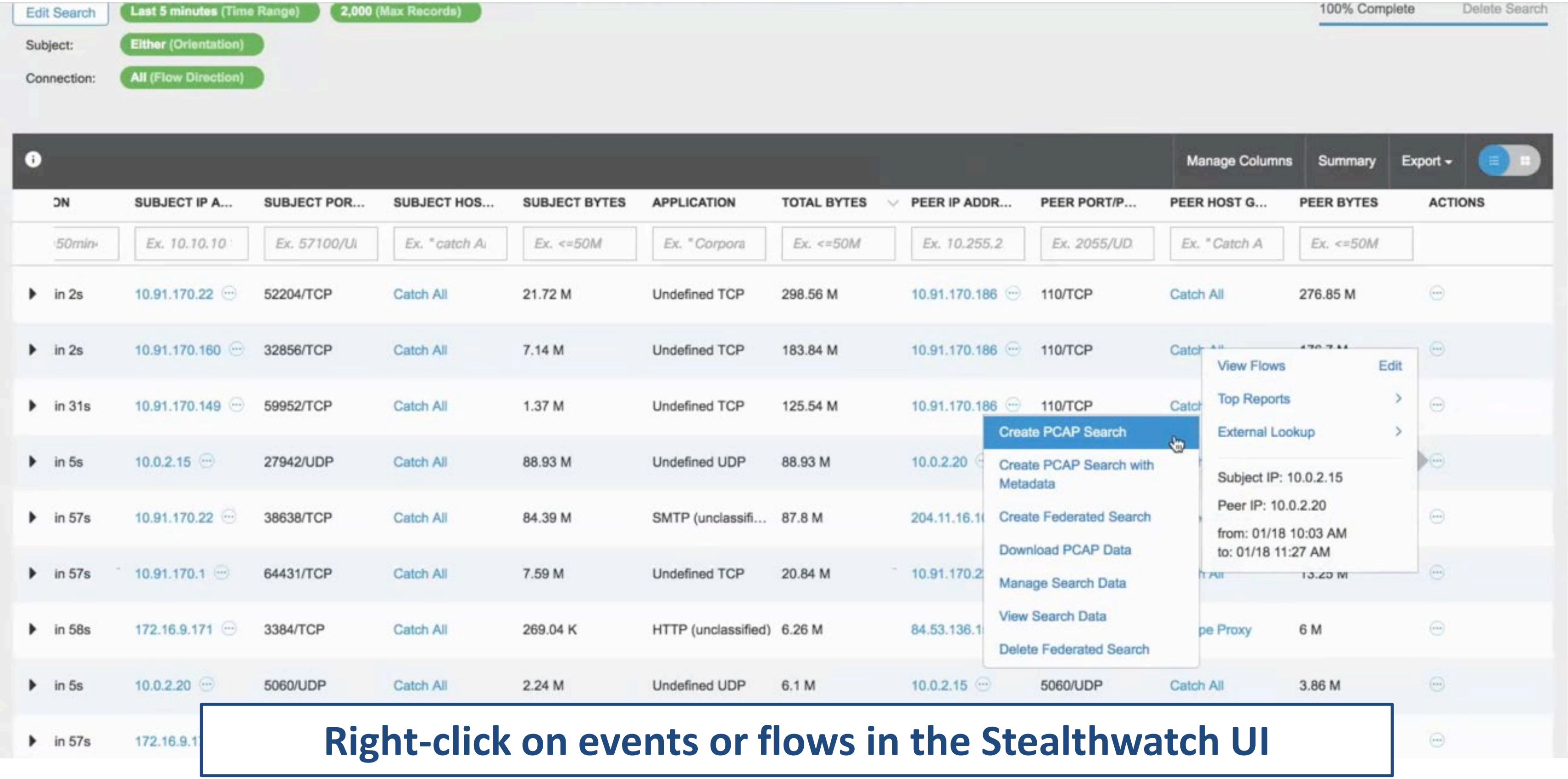
Pivot-to-PCAP from:

- Cisco Stealthwatch Console
- Cisco Firepower Mgmt Center
- Or <u>any</u> event from Cisco, or 3rd parties

REMOTE VIEWS + ITERATIVE SEARCH

- Global Data Exploration with Kibana
- Follow Streams & Suspicious Augmentation Alerts
- View/Analyze Packets
- Preview Objects/Files, MD5 malware, etc
- Generate Reports

Cisco Security Workflow – User pivot from any Stealthwatch event or flow, via the Packet Continuum connector

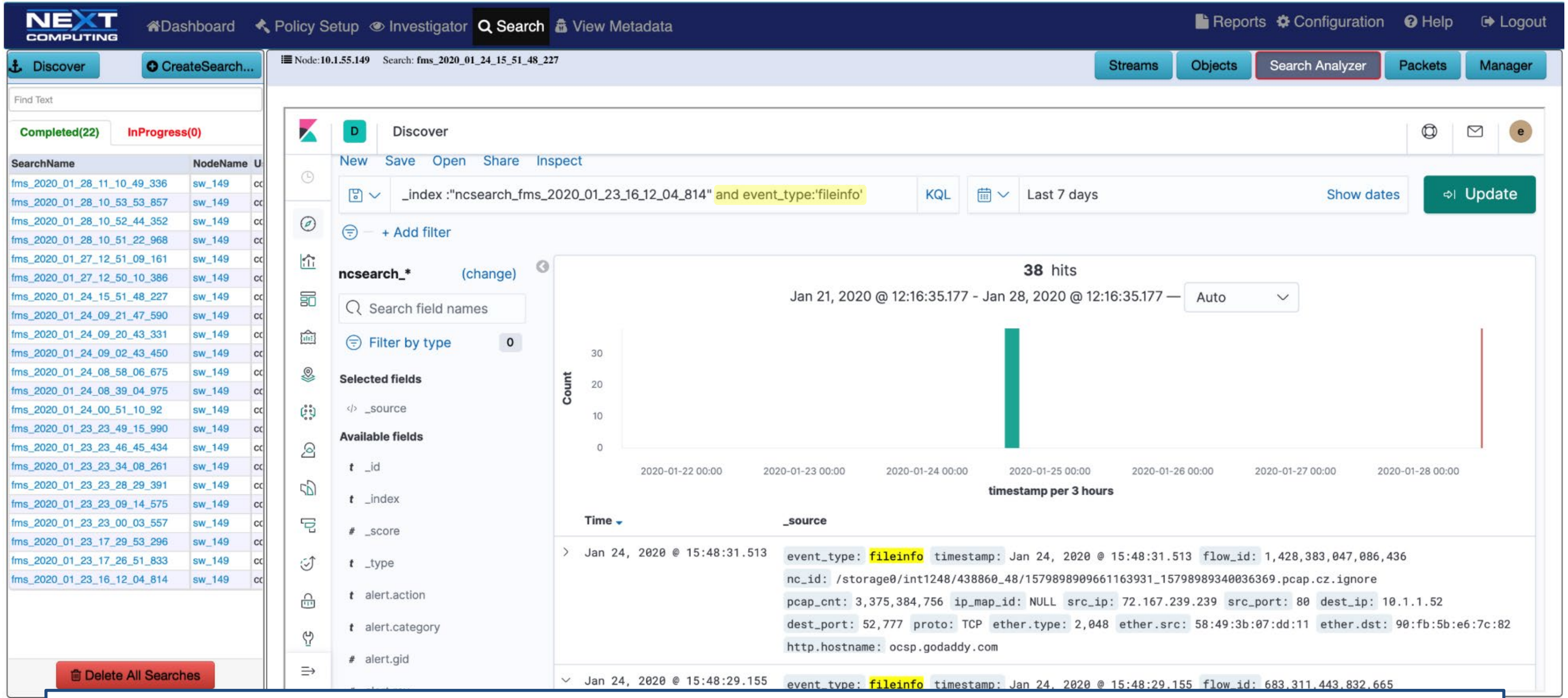


Subject IP: 10.0.2.15
Peer IP: 10.0.2.20
from: 01/18 10:03 AM
to: 01/18 11:27 AM

ON	SUBJECT IP A...	SUBJECT POR...	SUBJECT HOS...	SUBJECT BYTES	APPLICATION	TOTAL BYTES	PEER IP ADDR...	PEER PORT/P...	PEER HOST G...	PEER BYTES	ACTIONS
50min	Ex. 10.10.10	Ex. 57100/U	Ex. "catch A	Ex. <=50M	Ex. "Corpora	Ex. <=50M	Ex. 10.255.2	Ex. 2055/UD	Ex. "Catch A	Ex. <=50M	
in 2s	10.91.170.22	52204/TCP	Catch All	21.72 M	Undefined TCP	298.56 M	10.91.170.186	110/TCP	Catch All	276.85 M	
in 2s	10.91.170.160	32856/TCP	Catch All	7.14 M	Undefined TCP	183.84 M	10.91.170.186	110/TCP	Catch		
in 31s	10.91.170.149	59952/TCP	Catch All	1.37 M	Undefined TCP	125.54 M	10.91.170.186	110/TCP	Catch		
in 5s	10.0.2.15	27942/UDP	Catch All	88.93 M	Undefined UDP	88.93 M	10.0.2.20				
in 57s	10.91.170.22	38638/TCP	Catch All	84.39 M	SMTP (unclassifi...	87.8 M	204.11.16.1				
in 57s	10.91.170.1	64431/TCP	Catch All	7.59 M	Undefined TCP	20.84 M	10.91.170.2		h All	13.25 M	
in 58s	172.16.9.171	3384/TCP	Catch All	269.04 K	HTTP (unclassified)	6.26 M	84.53.136.1		pe Proxy	6 M	
in 5s	10.0.2.20	5060/UDP	Catch All	2.24 M	Undefined UDP	6.1 M	10.0.2.15	5060/UDP	Catch All	3.86 M	
in 57s	172.16.9.1										

Right-click on events or flows in the Stealthwatch UI

Investigator Workflow - Forensics investigations for a Stealthwatch pivot to explore the event, augmented by other critical alerts & logs



Node:10.1.55.149 Search: fms_2020_01_24_15_51_48_227

SearchName	NodeName	U
fms_2020_01_28_11_10_49_336	sw_149	cc
fms_2020_01_28_10_53_53_857	sw_149	cc
fms_2020_01_28_10_52_44_352	sw_149	cc
fms_2020_01_28_10_51_22_968	sw_149	cc
fms_2020_01_27_12_51_09_161	sw_149	cc
fms_2020_01_27_12_50_10_386	sw_149	cc
fms_2020_01_24_15_51_48_227	sw_149	cc
fms_2020_01_24_09_21_47_590	sw_149	cc
fms_2020_01_24_09_20_43_331	sw_149	cc
fms_2020_01_24_09_02_43_450	sw_149	cc
fms_2020_01_24_08_58_06_675	sw_149	cc
fms_2020_01_24_08_39_04_975	sw_149	cc
fms_2020_01_24_00_51_10_92	sw_149	cc
fms_2020_01_23_23_49_15_990	sw_149	cc
fms_2020_01_23_23_46_45_434	sw_149	cc
fms_2020_01_23_23_34_08_261	sw_149	cc
fms_2020_01_23_23_28_29_391	sw_149	cc
fms_2020_01_23_23_09_14_575	sw_149	cc
fms_2020_01_23_23_00_03_557	sw_149	cc
fms_2020_01_23_17_29_53_296	sw_149	cc
fms_2020_01_23_17_26_51_833	sw_149	cc
fms_2020_01_23_16_12_04_814	sw_149	cc

```
_index :"ncsearch_fms_2020_01_23_16_12_04_814" and event_type:'fileinfo'
```

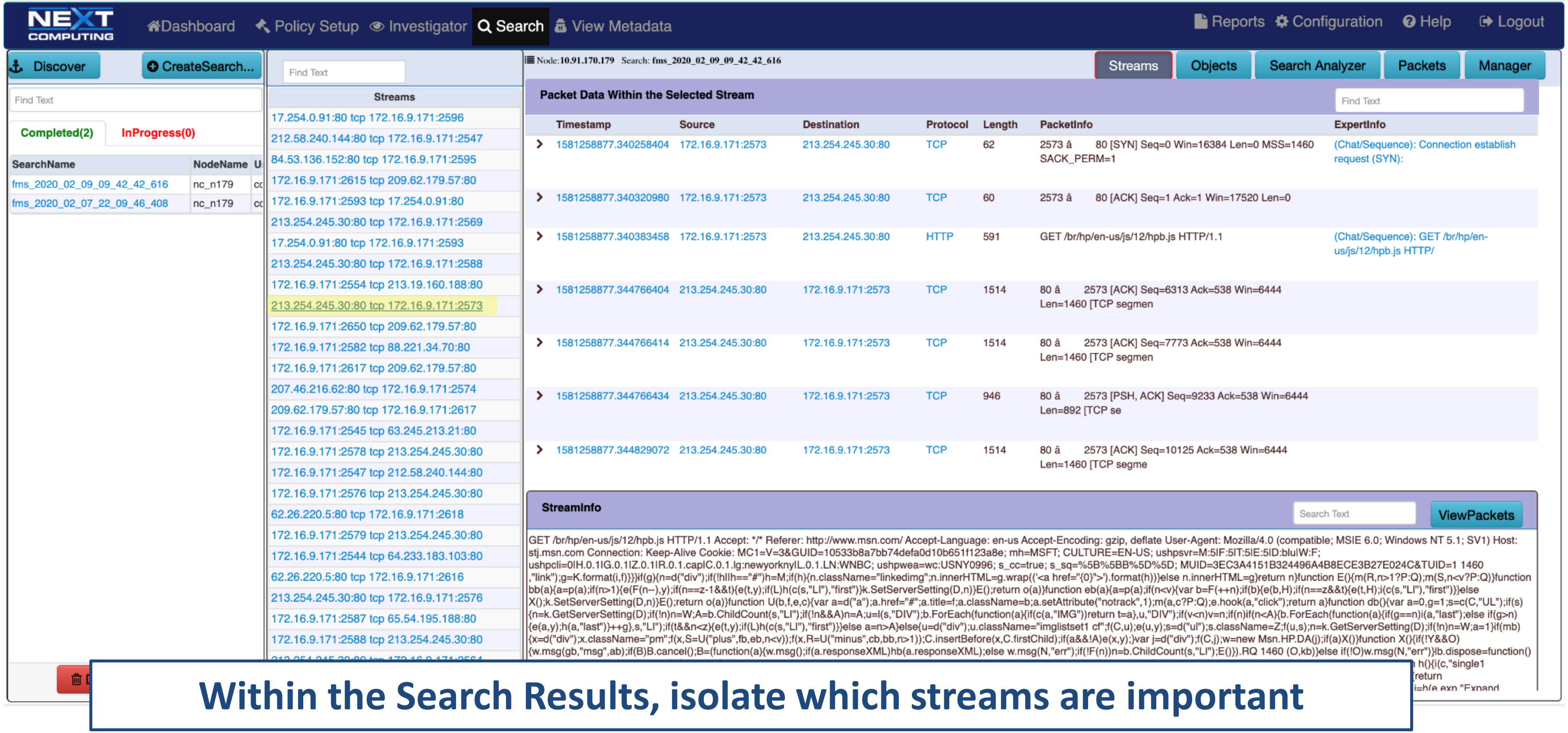
38 hits

Jan 21, 2020 @ 12:16:35.177 - Jan 28, 2020 @ 12:16:35.177 —

```
Time                       _source
> Jan 24, 2020 @ 15:48:31.513   event_type: fileinfo timestamp: Jan 24, 2020 @ 15:48:31.513 flow_id: 1,428,383,047,086,436
                                nc_id: /storage0/int1248/438860_48/1579898909661163931_15798989340036369.pcap.cz.ignore
                                pcap_cnt: 3,375,384,756 ip_map_id: NULL src_ip: 72.167.239.239 src_port: 80 dest_ip: 10.1.1.52
                                dest_port: 52,777 proto: TCP ether.type: 2,048 ether.src: 58:49:3b:07:dd:11 ether.dst: 90:fb:5b:e6:7c:82
                                http.hostname: ocsp.godaddy.com
∨ Jan 24, 2020 @ 15:48:29.155   event_type: fileinfo timestamp: Jan 24, 2020 @ 15:48:29.155 flow_id: 683,311,443,832,665
```

Pivot Search Results: Investigator allows user to refine search, eg. by file-type

Follow-the-Stream Workflow - for a Forensics Investigation
isolating bi-directional streams within overall search results



SearchName	NodeName	U
fms_2020_02_09_09_42_42_616	nc_n179	cc
fms_2020_02_07_22_09_46_408	nc_n179	cc

Streams
17.254.0.91:80 tcp 172.16.9.171:2596
212.58.240.144:80 tcp 172.16.9.171:2547
84.53.136.152:80 tcp 172.16.9.171:2595
172.16.9.171:2615 tcp 209.62.179.57:80
172.16.9.171:2593 tcp 17.254.0.91:80
213.254.245.30:80 tcp 172.16.9.171:2569
17.254.0.91:80 tcp 172.16.9.171:2593
213.254.245.30:80 tcp 172.16.9.171:2588
172.16.9.171:2554 tcp 213.19.160.188:80
213.254.245.30:80 tcp 172.16.9.171:2573
172.16.9.171:2650 tcp 209.62.179.57:80
172.16.9.171:2582 tcp 88.221.34.70:80
172.16.9.171:2617 tcp 209.62.179.57:80
207.46.216.62:80 tcp 172.16.9.171:2574
209.62.179.57:80 tcp 172.16.9.171:2617
172.16.9.171:2545 tcp 63.245.213.21:80
172.16.9.171:2578 tcp 213.254.245.30:80
172.16.9.171:2547 tcp 212.58.240.144:80
172.16.9.171:2576 tcp 213.254.245.30:80
62.26.220.5:80 tcp 172.16.9.171:2618
172.16.9.171:2579 tcp 213.254.245.30:80
172.16.9.171:2544 tcp 64.233.183.103:80
62.26.220.5:80 tcp 172.16.9.171:2616
213.254.245.30:80 tcp 172.16.9.171:2576
172.16.9.171:2587 tcp 65.54.195.188:80
172.16.9.171:2588 tcp 213.254.245.30:80

Node:10.91.170.179 Search: fms_2020_02_09_09_42_42_616

Packet Data Within the Selected Stream

Timestamp	Source	Destination	Protocol	Length	PacketInfo	ExpertInfo
1581258877.340258404	172.16.9.171:2573	213.254.245.30:80	TCP	62	2573 â 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1	(Chat/Sequence): Connection establish request (SYN):
1581258877.340320980	172.16.9.171:2573	213.254.245.30:80	TCP	60	2573 â 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0	
1581258877.340383458	172.16.9.171:2573	213.254.245.30:80	HTTP	591	GET /br/hp/en-us/js/12/hpb.js HTTP/1.1	(Chat/Sequence): GET /br/hp/en-us/js/12/hpb.js HTTP/
1581258877.344766404	213.254.245.30:80	172.16.9.171:2573	TCP	1514	80 â 2573 [ACK] Seq=6313 Ack=538 Win=6444 Len=1460 [TCP segmen	
1581258877.344766414	213.254.245.30:80	172.16.9.171:2573	TCP	1514	80 â 2573 [ACK] Seq=7773 Ack=538 Win=6444 Len=1460 [TCP segmen	
1581258877.344766434	213.254.245.30:80	172.16.9.171:2573	TCP	946	80 â 2573 [PSH, ACK] Seq=9233 Ack=538 Win=6444 Len=892 [TCP se	
1581258877.344829072	213.254.245.30:80	172.16.9.171:2573	TCP	1514	80 â 2573 [ACK] Seq=10125 Ack=538 Win=6444 Len=1460 [TCP segme	

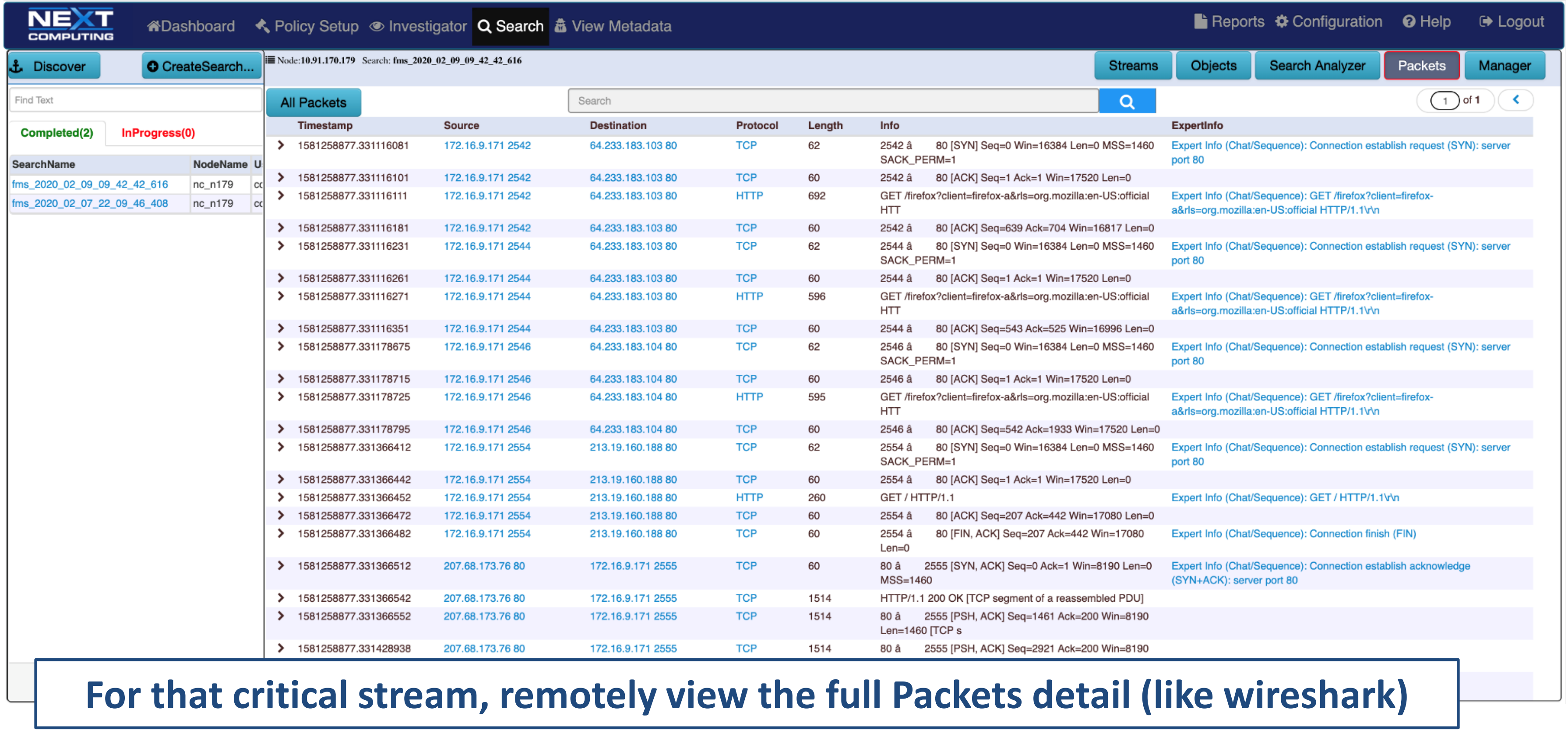
StreamInfo

```
GET /br/hp/en-us/js/12/hpb.js HTTP/1.1 Accept: */* Referer: http://www.msn.com/ Accept-Language: en-us Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) Host:
stj.msn.com Connection: Keep-Alive Cookie: MC1=V=3&GUID=10533b8a7bb74defa0d10b651f123a8e; mh=MSFT; CULTURE=EN-US; ushpsvr=M:5IF:5IT:5IE:5ID:bluIW:F;
ushpcli=0IH.0.1IG.0.1IZ.0.1IR.0.1.capIC.0.1.lg:newyorknyIL.0.1.LN:WNBC; ushpwea=wc:USNY0996; s_cc=true; s_sq=%5B%5BB%5D%5D; MUID=3EC3A4151B324496A4B8ECE3B27E024C&TUID=1 1460
,"link");g=K.format(i,f)}}}if(g){n=d("div");if(!hlIh=="#")h=M;if(h){n.className="linkedimg";n.innerHTML=g.wrap(('<a href="{0}">').format(h))}else n.innerHTML=g}return n}function E(){m(R,n>1?P:Q);m(S,n<v?P:Q)}function
bb(a){a=p(a);if(n>1){e(F(n--),y);if(n==z-1&&t){e(t,y);if(L)h(c(s,"LI"),"first")}k.SetServerSetting(D,n)}E();return o(a)}function eb(a){a=p(a);if(n<v){var b=F(++n);if(b){e(b,H);if(n==z&&t){e(t,H);i(c(s,"LI"),"first")}}else
X();k.SetServerSetting(D,n)}E();return o(a)}function U(b,f,e,c){var a=d("a");a.href="#";a.title=f;a.className=b;a.setAttribute("notrack",1);m(a,c?P:Q);e.hook(a,"click");return a}function db(){var a=0,g=1;s=c(C,"UL");if(s)
{n=k.GetServerSetting(D);if(!n)n=W;A=b.ChildCount(s,"LI");if(!n&&A)n=A;u=l(s,"DIV");b.ForEach(function(a){if(c(a,"IMG"))return t=a},u,"DIV");if(v<n)v=n;if(n)if(n<A){b.ForEach(function(a){if(g==n)i(a,"last");else if(g>n)
{e(a,y);h(a,"last")}++g},s,"LI");if(t&&n<z){e(t,y);if(L)h(c(s,"LI"),"first")}}else a=n>A}else{u=d("div");u.className="imglistset1 cf";f(C,u);e(u,y);s=d("ul");s.className=Z;f(u,s);n=k.GetServerSetting(D);if(!n)n=W;a=1}if(mb)
{x=d("div");x.className="pm";f(x,S=U("plus",fb,eb,n<v));f(x,R=U("minus",cb,bb,n>1));C.insertBefore(x,C.firstChild);if(a&&!A)e(x,y);}var j=d("div");f(C,j);w=new Msn.HP.DA(j);if(a)X()}function X(){if(!Y&&O)
{w.msg(gb,"msg",ab);if(B)B.cancel();B=(function(a){w.msg();if(a.responseXML)hb(a.responseXML);else w.msg(N,"err");if(!F(n))n=b.ChildCount(s,"LI");E()}).RQ 1460 (O,kb)}else if(!O)w.msg(N,"err")}lb.dispose=function()
h(){i(c,"single1
(return
i=h(e.exp,"Expand
```

Within the Search Results, isolate which streams are important

Follow-the-Stream Workflow - for a Forensics Investigation

isolating bi-directional streams within overall search results



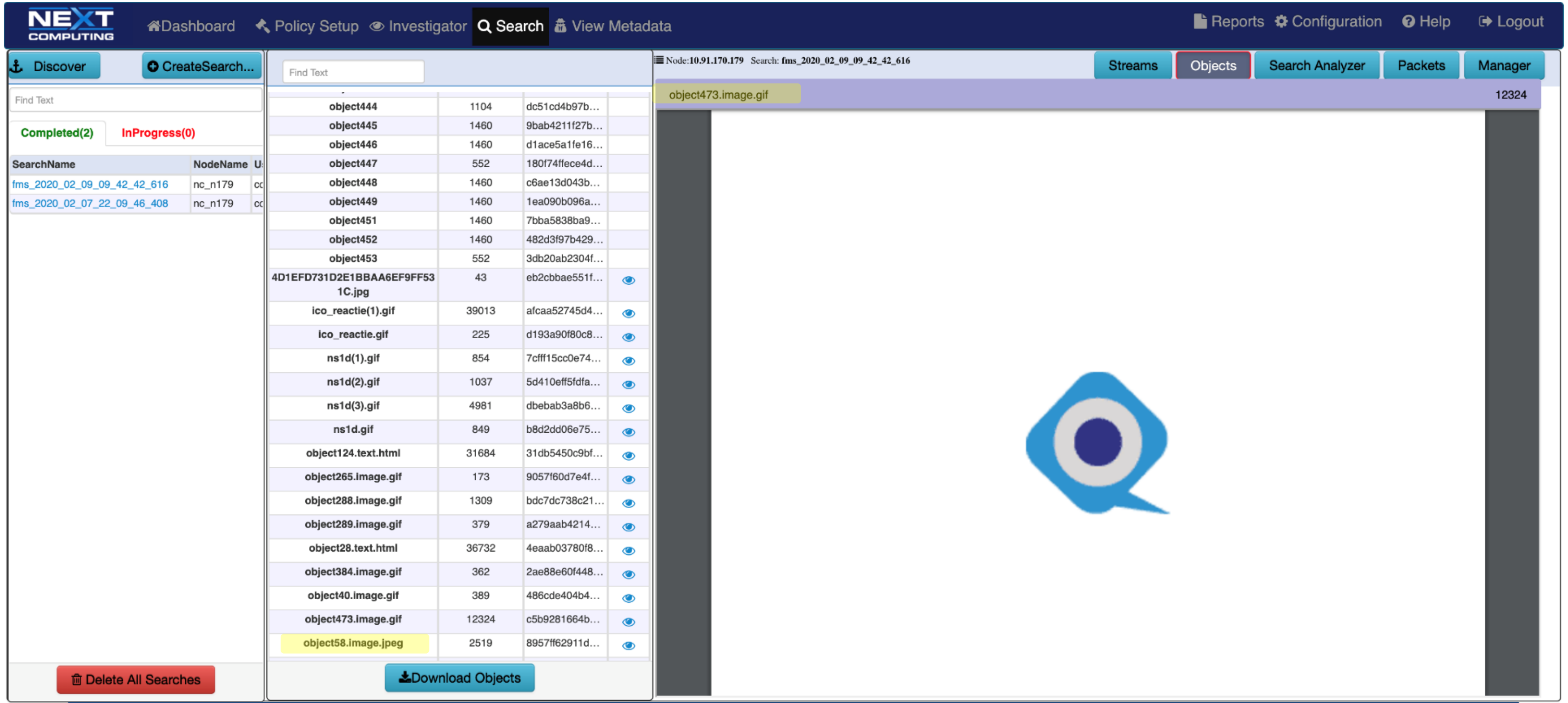
Node:10.91.170.179 Search: fms_2020_02_09_09_42_42_616

SearchName	NodeName	U
fms_2020_02_09_09_42_42_616	nc_n179	cc
fms_2020_02_07_22_09_46_408	nc_n179	cc

Timestamp	Source	Destination	Protocol	Length	Info	ExpertInfo
1581258877.331116081	172.16.9.171 2542	64.233.183.103 80	TCP	62	2542 â 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1	Expert Info (Chat/Sequence): Connection establish request (SYN): server port 80
1581258877.331116101	172.16.9.171 2542	64.233.183.103 80	TCP	60	2542 â 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0	
1581258877.331116111	172.16.9.171 2542	64.233.183.103 80	HTTP	692	GET /firefox?client=firefox-a&rls=org.mozilla:en-US:official HTT	Expert Info (Chat/Sequence): GET /firefox?client=firefox-a&rls=org.mozilla:en-US:official HTTP/1.1\r\n
1581258877.331116181	172.16.9.171 2542	64.233.183.103 80	TCP	60	2542 â 80 [ACK] Seq=639 Ack=704 Win=16817 Len=0	
1581258877.331116231	172.16.9.171 2544	64.233.183.103 80	TCP	62	2544 â 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1	Expert Info (Chat/Sequence): Connection establish request (SYN): server port 80
1581258877.331116261	172.16.9.171 2544	64.233.183.103 80	TCP	60	2544 â 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0	
1581258877.331116271	172.16.9.171 2544	64.233.183.103 80	HTTP	596	GET /firefox?client=firefox-a&rls=org.mozilla:en-US:official HTT	Expert Info (Chat/Sequence): GET /firefox?client=firefox-a&rls=org.mozilla:en-US:official HTTP/1.1\r\n
1581258877.331116351	172.16.9.171 2544	64.233.183.103 80	TCP	60	2544 â 80 [ACK] Seq=543 Ack=525 Win=16996 Len=0	
1581258877.331178675	172.16.9.171 2546	64.233.183.104 80	TCP	62	2546 â 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1	Expert Info (Chat/Sequence): Connection establish request (SYN): server port 80
1581258877.331178715	172.16.9.171 2546	64.233.183.104 80	TCP	60	2546 â 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0	
1581258877.331178725	172.16.9.171 2546	64.233.183.104 80	HTTP	595	GET /firefox?client=firefox-a&rls=org.mozilla:en-US:official HTT	Expert Info (Chat/Sequence): GET /firefox?client=firefox-a&rls=org.mozilla:en-US:official HTTP/1.1\r\n
1581258877.331178795	172.16.9.171 2546	64.233.183.104 80	TCP	60	2546 â 80 [ACK] Seq=542 Ack=1933 Win=17520 Len=0	
1581258877.331366412	172.16.9.171 2554	213.19.160.188 80	TCP	62	2554 â 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1	Expert Info (Chat/Sequence): Connection establish request (SYN): server port 80
1581258877.331366442	172.16.9.171 2554	213.19.160.188 80	TCP	60	2554 â 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0	
1581258877.331366452	172.16.9.171 2554	213.19.160.188 80	HTTP	260	GET / HTTP/1.1	Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n
1581258877.331366472	172.16.9.171 2554	213.19.160.188 80	TCP	60	2554 â 80 [ACK] Seq=207 Ack=442 Win=17080 Len=0	
1581258877.331366482	172.16.9.171 2554	213.19.160.188 80	TCP	60	2554 â 80 [FIN, ACK] Seq=207 Ack=442 Win=17080 Len=0	Expert Info (Chat/Sequence): Connection finish (FIN)
1581258877.331366512	207.68.173.76 80	172.16.9.171 2555	TCP	60	80 â 2555 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1460	Expert Info (Chat/Sequence): Connection establish acknowledge (SYN+ACK): server port 80
1581258877.331366542	207.68.173.76 80	172.16.9.171 2555	TCP	1514	HTTP/1.1 200 OK [TCP segment of a reassembled PDU]	
1581258877.331366552	207.68.173.76 80	172.16.9.171 2555	TCP	1514	80 â 2555 [PSH, ACK] Seq=1461 Ack=200 Win=8190 Len=1460 [TCP s	
1581258877.331428938	207.68.173.76 80	172.16.9.171 2555	TCP	1514	80 â 2555 [PSH, ACK] Seq=2921 Ack=200 Win=8190	

For that critical stream, remotely view the full Packets detail (like wireshark)

Follow-the-Stream Workflow - for a Forensics Investigation isolating bi-directional streams within overall search results



SearchName	NodeName	U
fms_2020_02_09_09_42_42_616	nc_n179	cc
fms_2020_02_07_22_09_46_408	nc_n179	cc

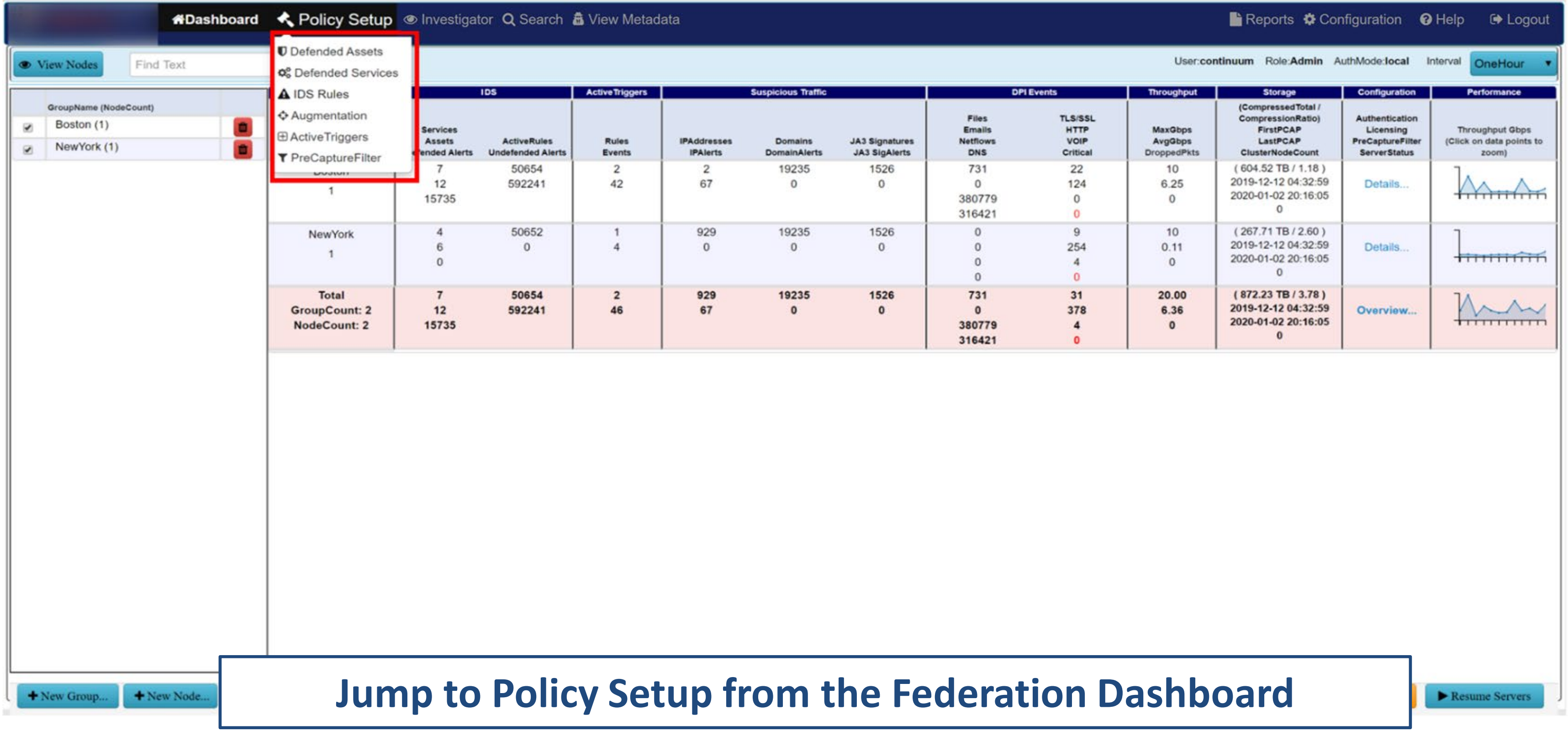
object444	1104	dc51cd4b97b...	
object445	1460	9bab4211f27b...	
object446	1460	d1ace5a1fe16...	
object447	552	180f74ffece4d...	
object448	1460	c6ae13d043b...	
object449	1460	1ea090b096a...	
object451	1460	7bba5838ba9...	
object452	1460	482d3f97b429...	
object453	552	3db20ab2304f...	
4D1EFD731D2E1BBAA6EF9FF531C.jpg	43	eb2cbbae551f...	👁
ico_reactie(1).gif	39013	afcaa52745d4...	👁
ico_reactie.gif	225	d193a90f80c8...	👁
ns1d(1).gif	854	7cfff15cc0e74...	👁
ns1d(2).gif	1037	5d410eff5fdfa...	👁
ns1d(3).gif	4981	dbebab3a8b6...	👁
ns1d.gif	849	b8d2dd06e75...	👁
object124.text.html	31684	31db5450c9bf...	👁
object265.image.gif	173	9057f60d7e4f...	👁
object288.image.gif	1309	bdc7dc738c21...	👁
object289.image.gif	379	a279aab4214...	👁
object28.text.html	36732	4eaab03780f8...	👁
object384.image.gif	362	2ae88e60f448...	👁
object40.image.gif	389	486cde404b4...	👁
object473.image.gif	12324	c5b9281664b...	👁
object58.image.jpeg	2519	8957ff62911d...	👁

Node:10.91.170.179 Search: fms_2020_02_09_09_42_42_616

object473.image.gif 12324

For that critical stream, remotely find and view the Objects, like this GIF file

Policy Update Workflow – Update user-defined alerts from new threat intel. The Federation will PUSH policies to ALL field appliances.



User:continuum Role:Admin AuthMode:local Interval OneHour

	GroupName (NodeCount)	
☑	Boston (1)	
☑	NewYork (1)	

	IDS		ActiveTriggers	Suspicious Traffic			DPI Events		Throughput	Storage	Configuration	Performance
	Services Assets ended Alerts	ActiveRules Undefended Alerts	Rules Events	IPAddresses IPAlerts	Domains DomainAlerts	JA3 Signatures JA3 SigAlerts	Files Emails Netflows DNS	TLS/SSL HTTP VOIP Critical	MaxGbps AvgGbps DroppedPkts	(CompressedTotal / CompressionRatio) FirstPCAP LastPCAP ClusterNodeCount	Authentication Licensing PreCaptureFilter ServerStatus	Throughput Gbps (Click on data points to zoom)
Boston 1	7 12 15735	50654 592241	2 42	2 67	19235 0	1526 0	731 0 380779 316421	22 124 0 0	10 6.25 0	(604.52 TB / 1.18) 2019-12-12 04:32:59 2020-01-02 20:16:05 0	Details...	
NewYork 1	4 6 0	50652 0	1 4	929 0	19235 0	1526 0	0 0 0 0	9 254 4 0	10 0.11 0	(267.71 TB / 2.60) 2019-12-12 04:32:59 2020-01-02 20:16:05 0	Details...	
Total GroupCount: 2 NodeCount: 2	**7 12 15735**	**50654 592241**	**2 46**	**929 67**	**19235 0**	**1526 0**	**731 0 380779 316421**	**31 378 4 0**	**20.00 6.36 0**	**(872.23 TB / 3.78) 2019-12-12 04:32:59 2020-01-02 20:16:05 0**	**Overview...**	

Jump to Policy Setup from the Federation Dashboard

Conclusion: Stealthwatch PCAP Use Cases

- **Use Steathwatch to initiate detailed Forensic IR Investigations**
  - Examine full lossless packet capture data of suspicious activity around any critical alert – over extended timeline periods
- **Supplement Stealthwatch with rich data augmentation around events**
  - Pivot from Stealthwatch into a full-featured Data Visualization Investigator
  - “What else is going around this critical event?”
  - Isolate & follow individual “Streams”, augmented with known suspicious files & activity like domains or JA3 signatures, in addition to user-defined IDS snort alerts, etc
- **Leverage valuable Stealthwatch alerting policies:**
  - Extend the timeline for critical data retention, beyond the lossless Capture Timeline
  - Retrospective Detection: Did similar behavior occur in the past, while undetected?
  - Trigger automated capture & extraction workflows