Key Take-Aways – Packet Continuum UCS

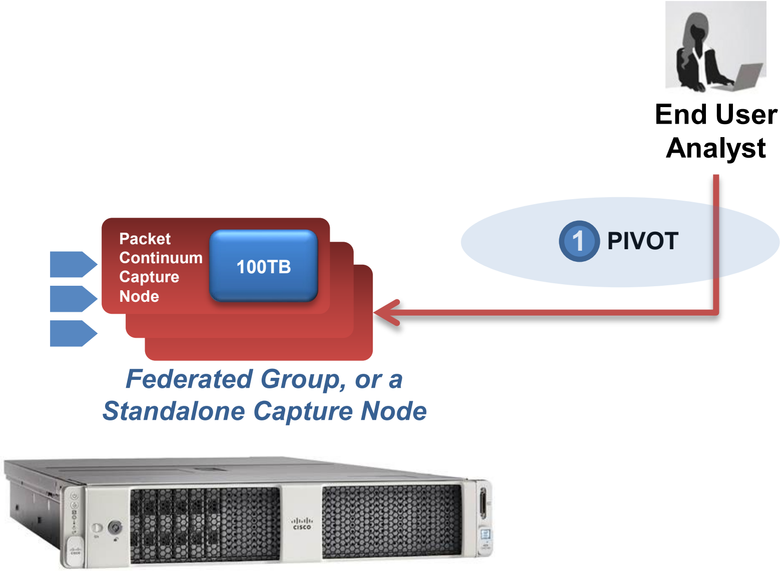
- **Easy Pivot-to-PCAP from Cisco Security events**
  - Easy workflow to Forensic IR Investigations, from Stealthwatch, FMC or any 3rd party event
  - Optimized for standard Cisco UCS servers, with UCS hardware credit to Cisco sellers
  - Field-upgrade for legacy CS Packet Analyzer appliances
- **Automated capture policies & workflows**
  - Event-related queries retain critical data, even beyond the ***lossless capture*** timeline period
  - Mature REST/API for easy workflow integrations, using open data access & standard interfaces
- **Low-cost entry-level options => Easy Proof-of-Concept**
- **Unique features for massive scale => Carrier-grade and large-enterprise networks**
  - Federated search across many capture nodes – up to 10,000
  - Very long capture timelines – weeks/months
  - Very high lossless capture rates – 300-500^{++}Gbps

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	

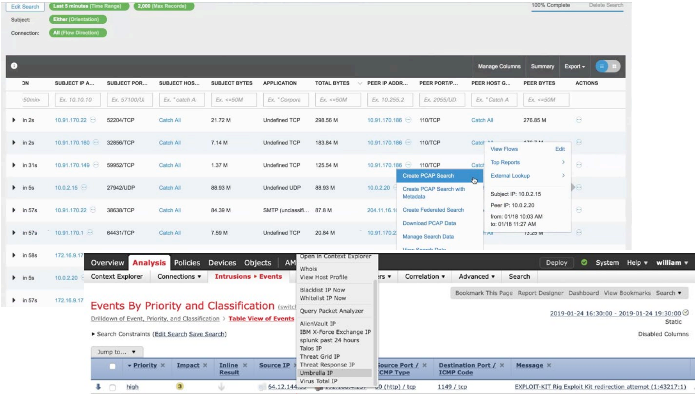
* NOTE: NextComputing's NextServer-X Portable/Deployable is a TSA-compliant carry-on (<35lbs) and also suitable for mobile deployment of virtualized Stealthwatch modules, with or without Packet Continuum software.

First, Pivot from Cisco Security



Federated Group, or a Standalone Capture Node

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


Edit Search
Last 5 minutes (Time Range)
2,000 (Max Records)
100% Complete
Delete Search
Subject: Either (Orientation)
Connection: All (Flow Direction)
Manage Columns
Summary
Export

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			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

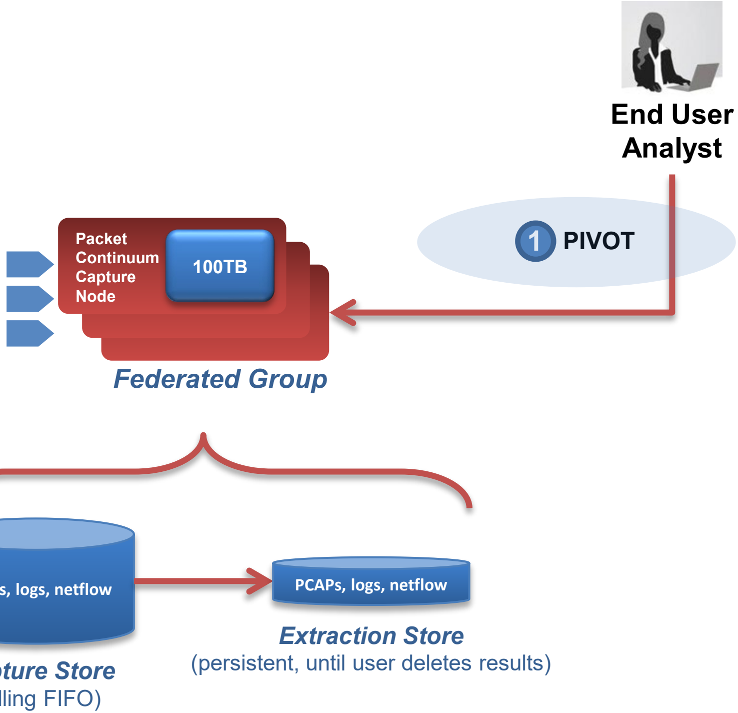
▸ Search Constraints (Edit Search Save Search)

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

Disabled Columns

	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)

Data Retention Workflow – Any Pivot/Search from Cisco Analytics save critical data, even beyond the lossless Capture Timeline period



End User Analyst

1 PIVOT

Packet Continuum Capture Node

100TB

Federated Group

PCAPs, logs, netflow

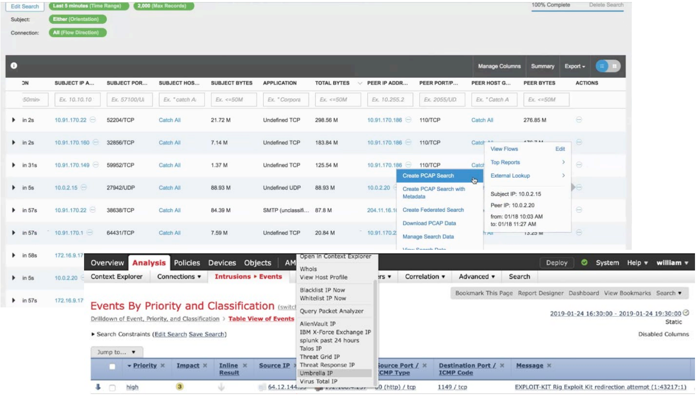
PCAPs, logs, netflow

Capture Store
(rolling FIFO)

Extraction Store
(persistent, until user deletes results)

Pivot-to-PCAP from:

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



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			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 (switc

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

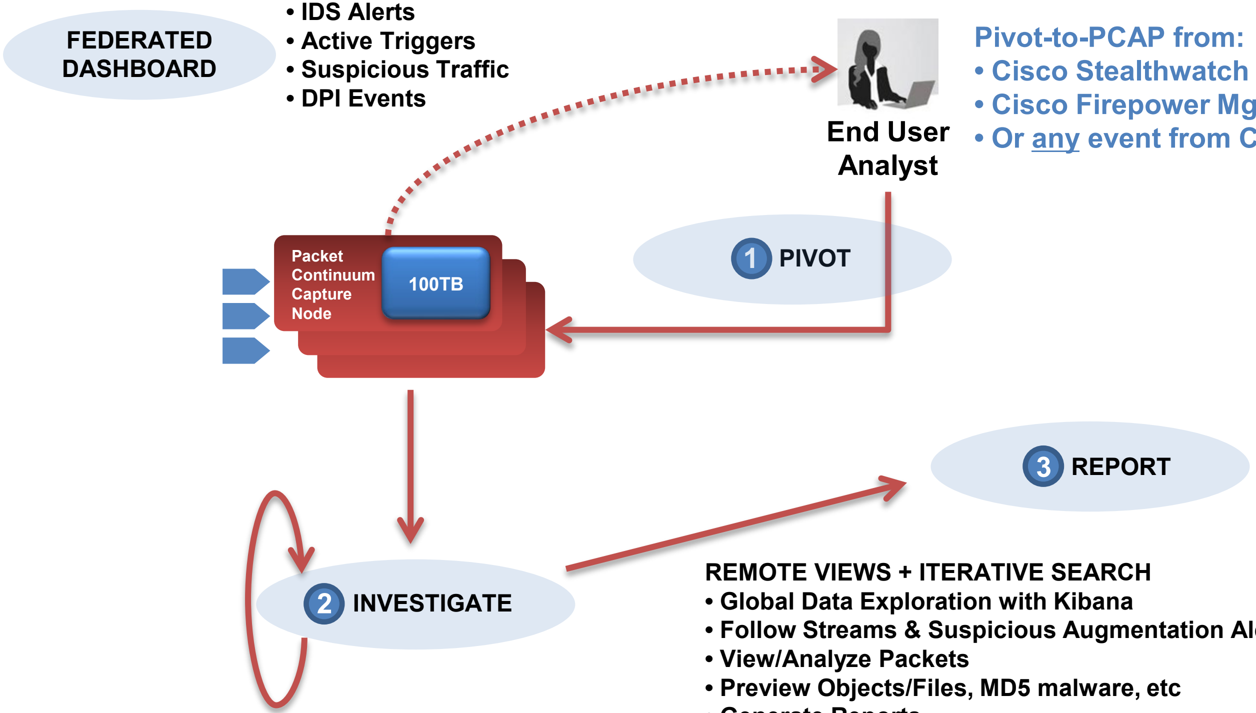
▸ Search Constraints (Edit Search Save Search)

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

Disabled Columns

	Priority	Impact	Inline Result	Source IP		ource Port / CMP Type	Destination Port / ICMP Code	Message
□	high	3		64.12.144.		0 (http) / tcp	1149 / tcp	EXPLOIT-KIT Rig Exploit Kit redirection attempt (1:43217:1)

Simplified PCAP Workflow: Summary



FEDERATED DASHBOARD

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

End User Analyst

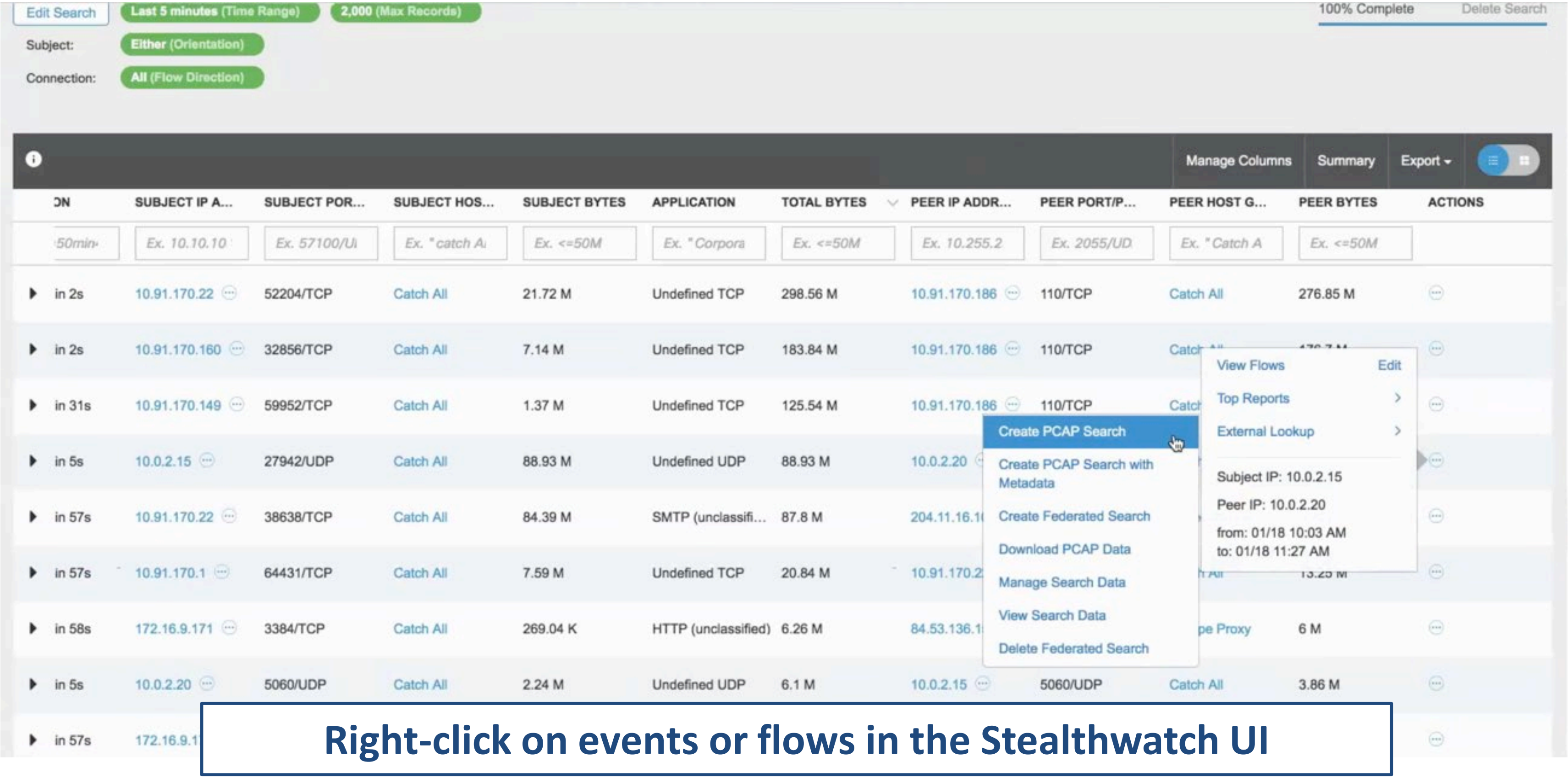
Pivot-to-PCAP from:

- Cisco Stealthwatch Console
- Cisco Firepower Mgmt Center
- Or any 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



Last 5 minutes (Time Range) | 2,000 (Max Records)

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	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										

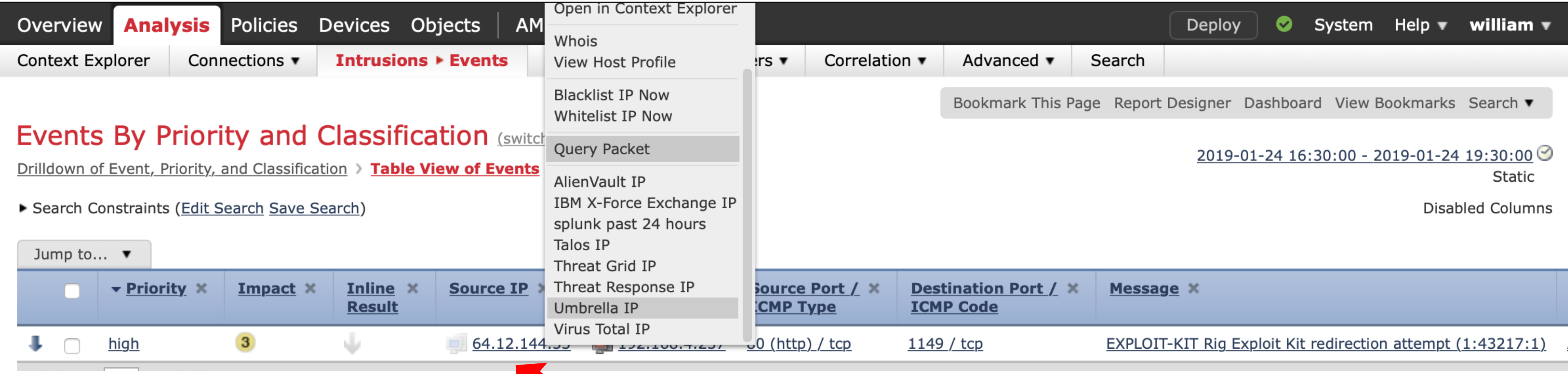
Subject IP: 10.0.2.15

Peer IP: 10.0.2.20

from: 01/18 10:03 AM
to: 01/18 11:27 AM

Right-click on events or flows in the Stealthwatch UI

Cisco Security Workflow – User pivot from any Firepower event, via the Packet Continuum connector



Events By Priority and Classification (switch

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

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

▸ Search Constraints (Edit Search Save Search)

Disabled Columns

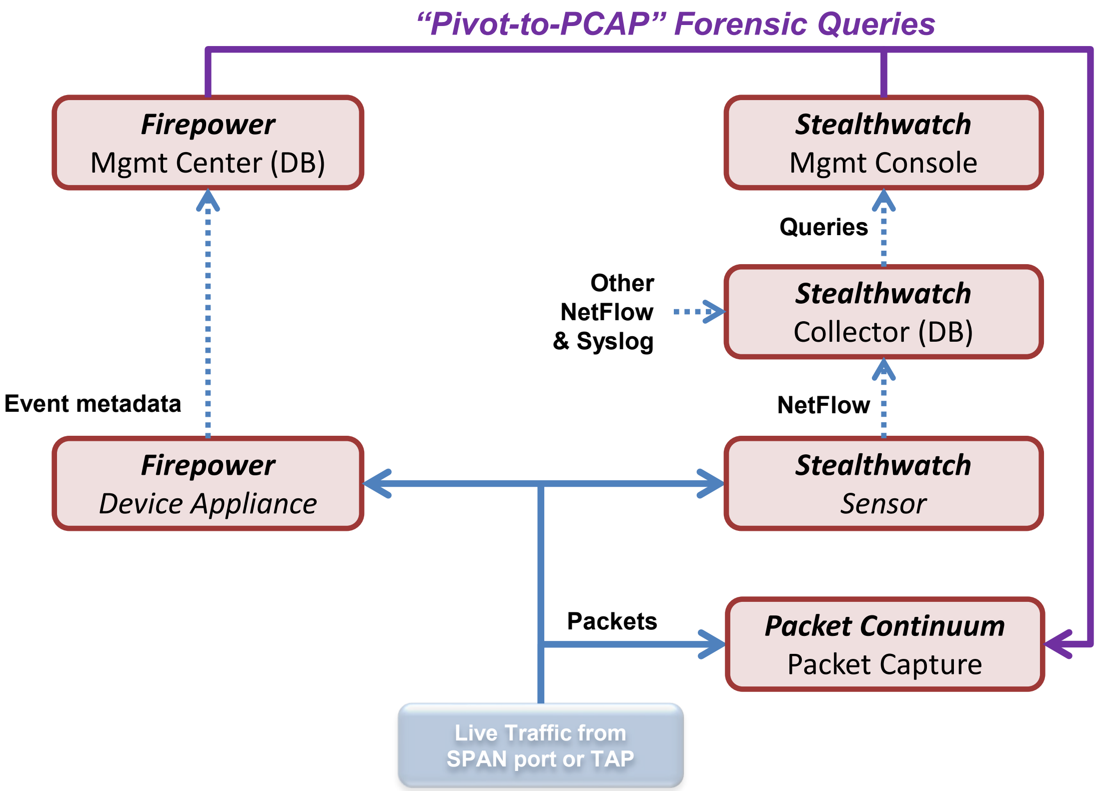
	□	Priority	Impact	Inline Result	Source IP		ource Port / CMP Type	Destination Port / ICMP Code	Message
⬇	□	high	3	↓	64.12.144.53	[illegible]	80 (http) / tcp	1149 / tcp	EXPLOIT-KIT Rig Exploit Kit redirection attempt (1:43217:1)

Right Click on a record and scroll down the menu

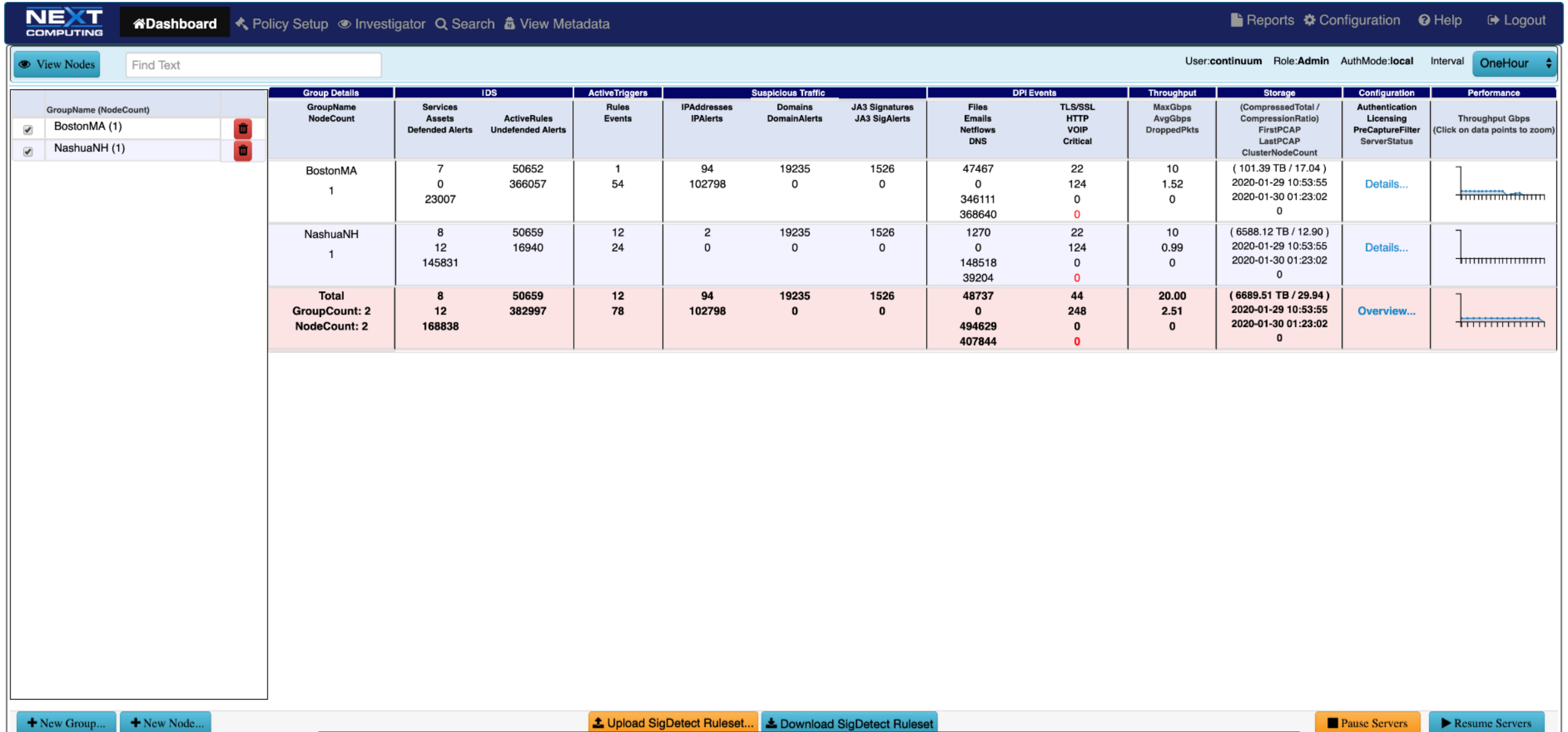
https://10.91.170.191/v1/createsearch?srchost=64.12.144.53

Right-click on events in the Firepower Management Center

Cisco Security PCAP Integrations



Federation Workflow - Federation and aggregation of capture nodes in different locations or within the same datacenter



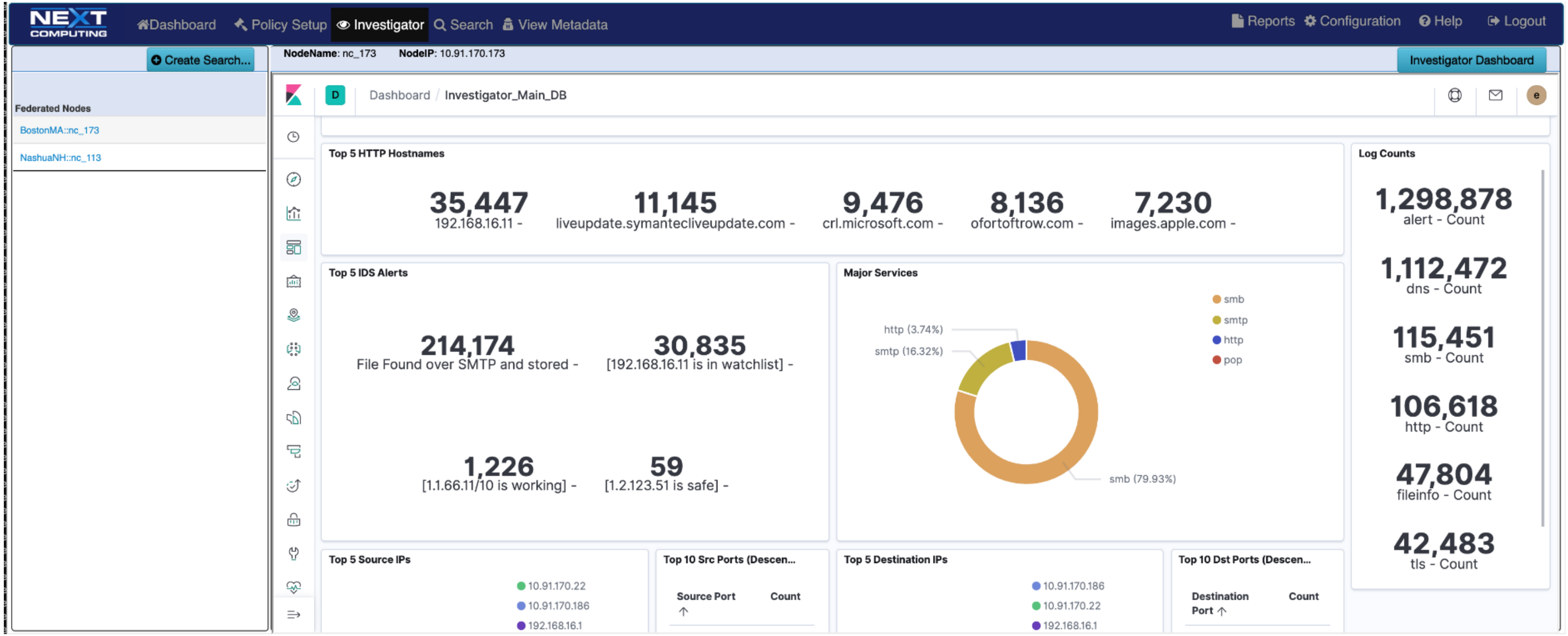
User:**continuum** Role:**Admin** AuthMode:**local** Interval OneHour

	GroupName (NodeCount)	
☑	BostonMA (1)	🗑
☑	NashuaNH (1)	🗑

Group Details	IDS		ActiveTriggers	Suspicious Traffic			DPI Events		Throughput	Storage	Configuration	Performance
GroupName NodeCount	Services Assets Defended 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)
BostonMA 1	7 0 23007	50652 366057	1 54	94 102798	19235 0	1526 0	47467 0 346111 368640	22 124 0 0	10 1.52 0	(101.39 TB / 17.04) 2020-01-29 10:53:55 2020-01-30 01:23:02 0	Details...	
NashuaNH 1	8 12 145831	50659 16940	12 24	2 0	19235 0	1526 0	1270 0 148518 39204	22 124 0 0	10 0.99 0	(6588.12 TB / 12.90) 2020-01-29 10:53:55 2020-01-30 01:23:02 0	Details...	
Total GroupCount: 2 NodeCount: 2	**8 12 168838**	**50659 382997**	**12 78**	**94 102798**	**19235 0**	**1526 0**	**48737 0 494629 407844**	**44 248 0 0**	**20.00 2.51 0**	**(6689.51 TB / 29.94) 2020-01-29 10:53:55 2020-01-30 01:23:02 0**	**Overview...**	

Federation Manager: Global Dashboard

Federation Workflow - Federation and aggregation of capture nodes in different locations or within the same datacenter



NodeName: nc_173 **NodeIP:** 10.91.170.173

Federated Nodes

- BostonMA::nc_173
- NashuaNH::nc_113

Top 5 HTTP Hostnames

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

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 IDS Alerts

214,174 File Found over SMTP and stored -
30,835 [192.168.16.11 is in watchlist] -
1,226 [1.1.66.11/10 is working] -
59 [1.2.123.51 is safe] -

Major Services

Top 5 Source IPs

● 10.91.170.22
● 10.91.170.186
● 192.168.16.1

Top 10 Src Ports (Descen...

Source Port ↑	Count

Top 5 Destination IPs

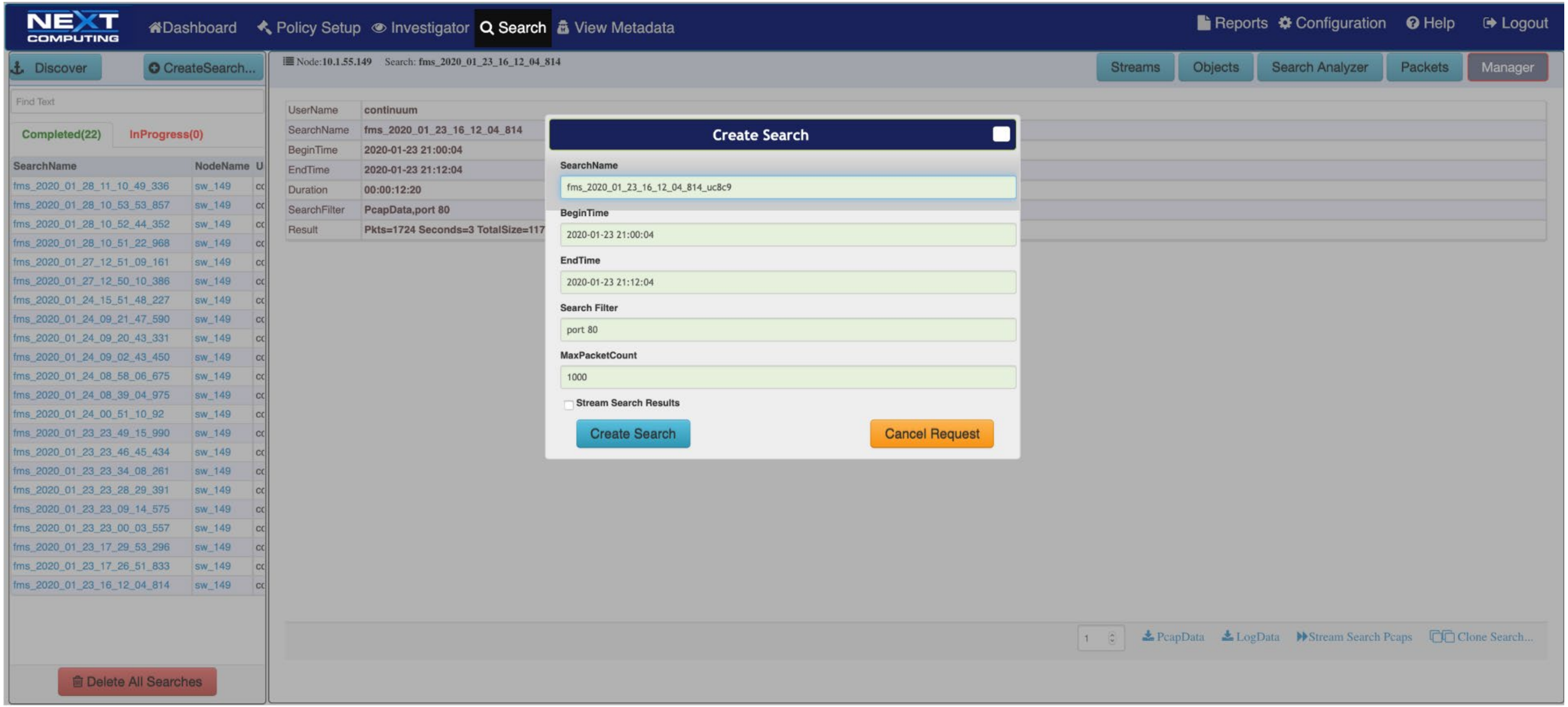
● 10.91.170.186
● 10.91.170.22
● 192.168.16.1

Top 10 Dst Ports (Descen...

Destination Port ↑	Count

Investigator: Global Dashboard

Search Workflow - Forensics investigations based on search or pivot from an alert in Cisco Stealthwatch



Completed(22) InProgress(0)

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

Node:10.1.55.149 Search: fms_2020_01_23_16_12_04_814

UserName	continuum
SearchName	fms_2020_01_23_16_12_04_814
BeginTime	2020-01-23 21:00:04
EndTime	2020-01-23 21:12:04
Duration	00:00:12:20
SearchFilter	PcapData,port 80
Result	Pkts=1724 Seconds=3 TotalSize=117

Create Search

SearchName: fms_2020_01_23_16_12_04_814_uc8c9

BeginTime: 2020-01-23 21:00:04

EndTime: 2020-01-23 21:12:04

Search Filter: port 80

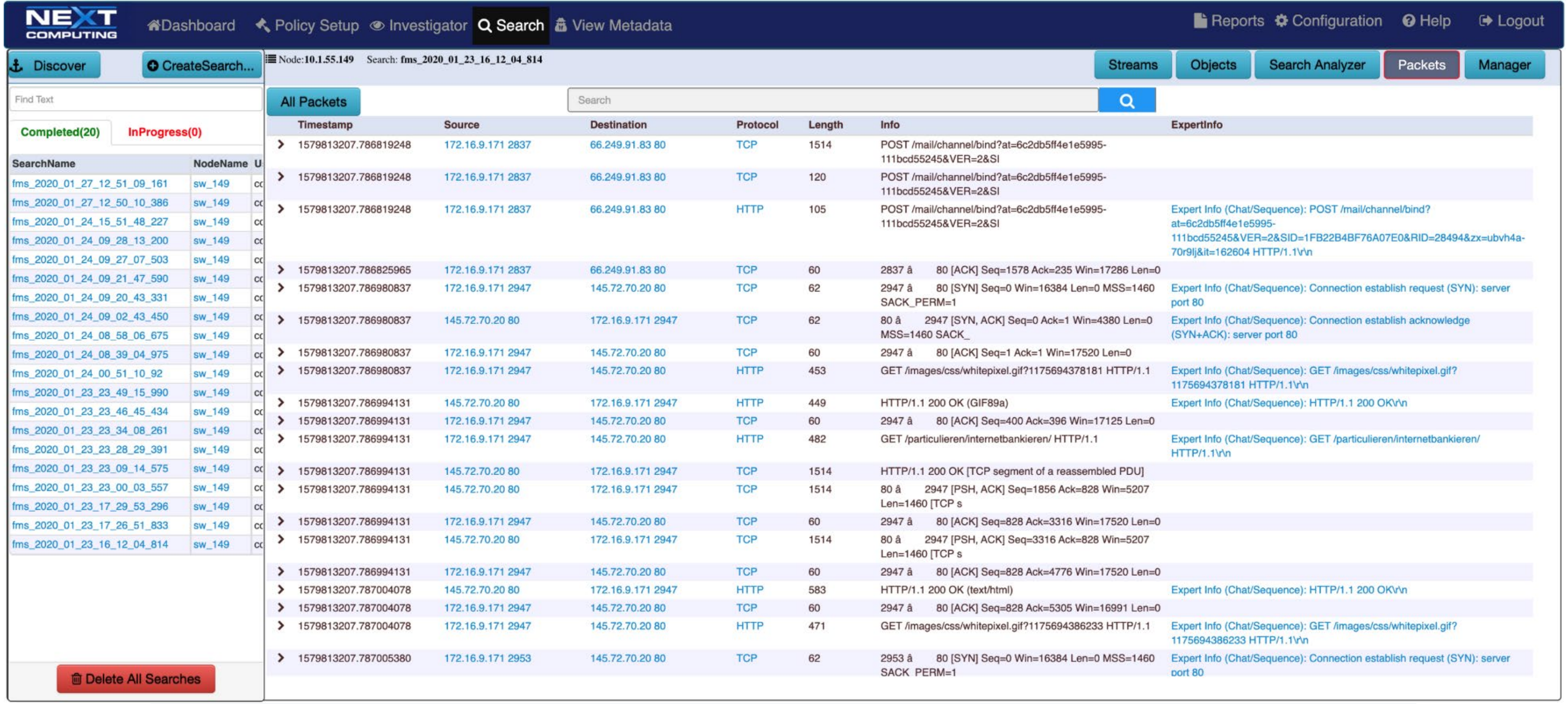
MaxPacketCount: 1000

□ Stream Search Results

Create Search   Cancel Request

Search Manager: Create Search

Search Workflow - Forensics investigations based on search or pivot from an alert in Cisco Stealthwatch



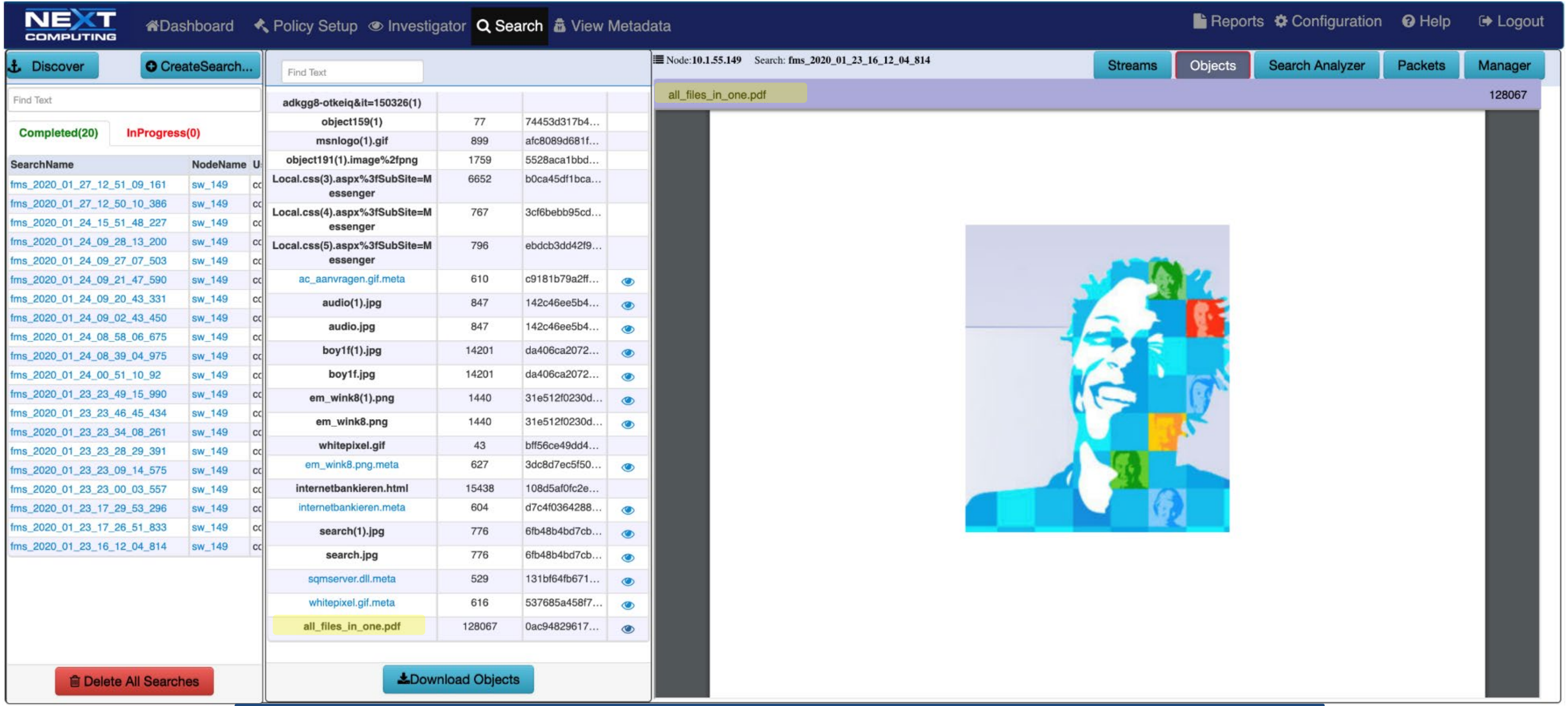
Node:10.1.55.149 Search: fms_2020_01_23_16_12_04_814

SearchName	NodeName	U
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_28_13_200	sw_149	cc
fms_2020_01_24_09_27_07_503	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

	Timestamp	Source	Destination	Protocol	Length	Info	ExpertInfo
>	1579813207.786819248	172.16.9.171 2837	66.249.91.83 80	TCP	1514	POST /mail/channel/bind?at=6c2db5ff4e1e5995-111bcd55245&VER=2&SI	
>	1579813207.786819248	172.16.9.171 2837	66.249.91.83 80	TCP	120	POST /mail/channel/bind?at=6c2db5ff4e1e5995-111bcd55245&VER=2&SI	
>	1579813207.786819248	172.16.9.171 2837	66.249.91.83 80	HTTP	105	POST /mail/channel/bind?at=6c2db5ff4e1e5995-111bcd55245&VER=2&SI	Expert Info (Chat/Sequence): POST /mail/channel/bind?at=6c2db5ff4e1e5995-111bcd55245&VER=2&SID=1FB22B4BF76A07E0&RID=28494&zx=ubvh4a-70r9lj&it=162604 HTTP/1.1\r\n
>	1579813207.786825965	172.16.9.171 2837	66.249.91.83 80	TCP	60	2837 â 80 [ACK] Seq=1578 Ack=235 Win=17286 Len=0	
>	1579813207.786980837	172.16.9.171 2947	145.72.70.20 80	TCP	62	2947 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
>	1579813207.786980837	145.72.70.20 80	172.16.9.171 2947	TCP	62	80 â 2947 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_	Expert Info (Chat/Sequence): Connection establish acknowledge (SYN+ACK): server port 80
>	1579813207.786980837	172.16.9.171 2947	145.72.70.20 80	TCP	60	2947 â 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0	
>	1579813207.786980837	172.16.9.171 2947	145.72.70.20 80	HTTP	453	GET /images/css/whitepixel.gif?1175694378181 HTTP/1.1	Expert Info (Chat/Sequence): GET /images/css/whitepixel.gif?1175694378181 HTTP/1.1\r\n
>	1579813207.786994131	145.72.70.20 80	172.16.9.171 2947	HTTP	449	HTTP/1.1 200 OK (GIF89a)	Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n
>	1579813207.786994131	172.16.9.171 2947	145.72.70.20 80	TCP	60	2947 â 80 [ACK] Seq=400 Ack=396 Win=17125 Len=0	
>	1579813207.786994131	172.16.9.171 2947	145.72.70.20 80	HTTP	482	GET /particulieren/internetbankieren/ HTTP/1.1	Expert Info (Chat/Sequence): GET /particulieren/internetbankieren/ HTTP/1.1\r\n
>	1579813207.786994131	145.72.70.20 80	172.16.9.171 2947	TCP	1514	HTTP/1.1 200 OK [TCP segment of a reassembled PDU]	
>	1579813207.786994131	145.72.70.20 80	172.16.9.171 2947	TCP	1514	80 â 2947 [PSH, ACK] Seq=1856 Ack=828 Win=5207 Len=1460 [TCP s	
>	1579813207.786994131	172.16.9.171 2947	145.72.70.20 80	TCP	60	2947 â 80 [ACK] Seq=828 Ack=3316 Win=17520 Len=0	
>	1579813207.786994131	145.72.70.20 80	172.16.9.171 2947	TCP	1514	80 â 2947 [PSH, ACK] Seq=3316 Ack=828 Win=5207 Len=1460 [TCP s	
>	1579813207.786994131	172.16.9.171 2947	145.72.70.20 80	TCP	60	2947 â 80 [ACK] Seq=828 Ack=4776 Win=17520 Len=0	
>	1579813207.787004078	145.72.70.20 80	172.16.9.171 2947	HTTP	583	HTTP/1.1 200 OK (text/html)	Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n
>	1579813207.787004078	172.16.9.171 2947	145.72.70.20 80	TCP	60	2947 â 80 [ACK] Seq=828 Ack=5305 Win=16991 Len=0	
>	1579813207.787004078	172.16.9.171 2947	145.72.70.20 80	HTTP	471	GET /images/css/whitepixel.gif?1175694386233 HTTP/1.1	Expert Info (Chat/Sequence): GET /images/css/whitepixel.gif?1175694386233 HTTP/1.1\r\n
>	1579813207.787005380	172.16.9.171 2953	145.72.70.20 80	TCP	62	2953 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

Search Results: Packets View, like a remote wireshark dashboard

Search Workflow - Forensics investigations based on search or pivot from an alert in Cisco Stealthwatch



Completed(20) InProgress(0)

SearchName	NodeName	U
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_28_13_200	sw_149	cc
fms_2020_01_24_09_27_07_503	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

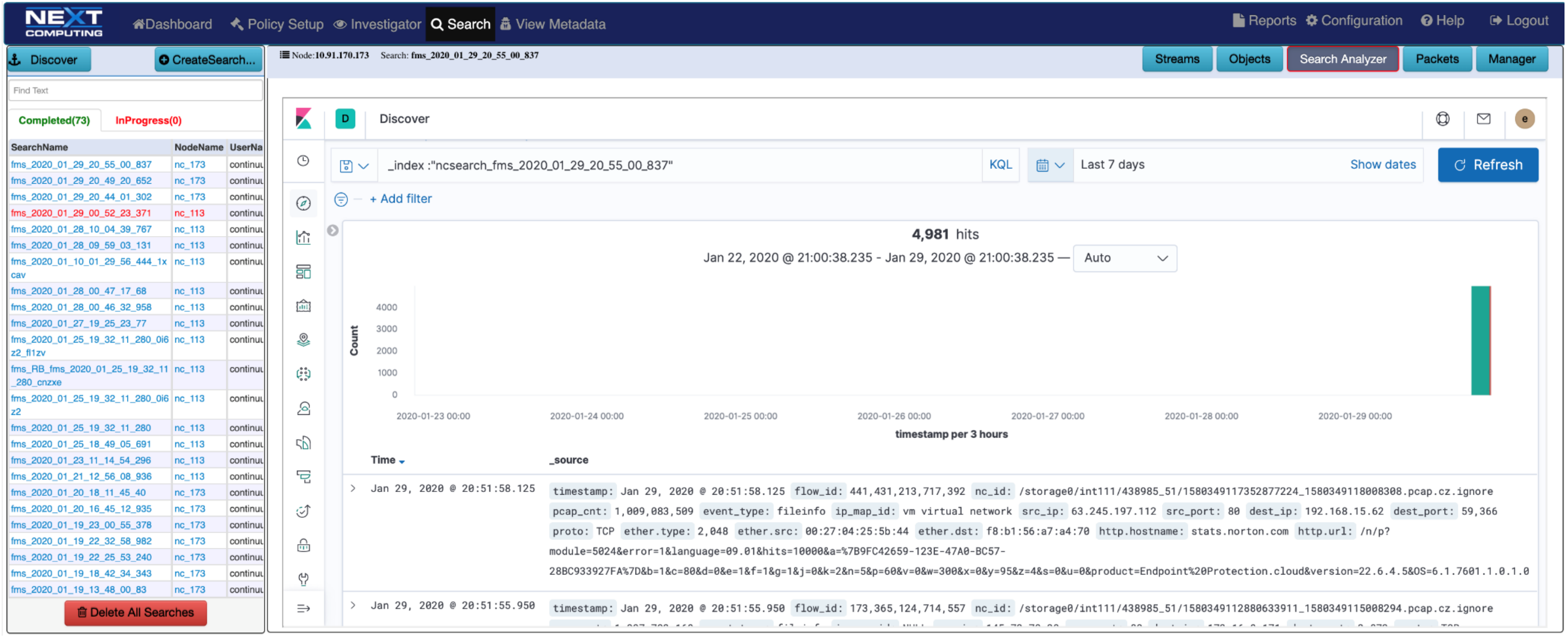
adkgg8-otkeiq&it=150326(1)			
object159(1)	77	74453d317b4...	
msnlogo(1).gif	899	afc8089d681f...	
object191(1).image%2fpng	1759	5528aca1bbd...	
Local.css(3).aspx%3fSubSite=Messenger	6652	b0ca45df1bca...	
Local.css(4).aspx%3fSubSite=Messenger	767	3cf6bebb95cd...	
Local.css(5).aspx%3fSubSite=Messenger	796	ebdcb3dd42f9...	
ac_aanvragen.gif.meta	610	c9181b79a2ff...	👁
audio(1).jpg	847	142c46ee5b4...	👁
audio.jpg	847	142c46ee5b4...	👁
boy1f(1).jpg	14201	da406ca2072...	👁
boy1f.jpg	14201	da406ca2072...	👁
em_wink8(1).png	1440	31e512f0230d...	👁
em_wink8.png	1440	31e512f0230d...	👁
whitepixel.gif	43	bff56ce49dd4...	
em_wink8.png.meta	627	3dc8d7ec5f50...	👁
internetbankieren.html	15438	108d5af0fc2e...	
internetbankieren.meta	604	d7c4f0364288...	👁
search(1).jpg	776	6fb48b4bd7cb...	👁
search.jpg	776	6fb48b4bd7cb...	👁
sqmserver.dll.meta	529	131bf64fb671...	👁
whitepixel.gif.meta	616	537685a458f7...	👁
all_files_in_one.pdf	128067	0ac94829617...	👁

Node: 10.1.55.149 Search: fms_2020_01_23_16_12_04_814

all_files_in_one.pdf 128067

Search Results: Object View, showing a PDF file

Search Workflow - Forensics investigations based on search or pivot from an alert in Cisco Stealthwatch



SearchName	NodeName	UserNa
fms_2020_01_29_20_55_00_837	nc_173	continuu
fms_2020_01_29_20_49_20_652	nc_173	continuu
fms_2020_01_29_20_44_01_302	nc_173	continuu
fms_2020_01_29_00_52_23_371	nc_113	continuu
fms_2020_01_28_10_04_39_767	nc_113	continuu
fms_2020_01_28_09_59_03_131	nc_113	continuu
fms_2020_01_10_01_29_56_444_1xcav	nc_113	continuu
fms_2020_01_28_00_47_17_68	nc_113	continuu
fms_2020_01_28_00_46_32_958	nc_113	continuu
fms_2020_01_27_19_25_23_77	nc_113	continuu
fms_2020_01_25_19_32_11_280_0i6z2_fl1zv	nc_113	continuu
fms_RB_fms_2020_01_25_19_32_11_280_cnzxe	nc_113	continuu
fms_2020_01_25_19_32_11_280_0i6z2	nc_113	continuu
fms_2020_01_25_19_32_11_280	nc_113	continuu
fms_2020_01_25_18_49_05_691	nc_113	continuu
fms_2020_01_23_11_14_54_296	nc_113	continuu
fms_2020_01_21_12_56_08_936	nc_113	continuu
fms_2020_01_20_18_11_45_40	nc_173	continuu
fms_2020_01_20_16_45_12_935	nc_173	continuu
fms_2020_01_19_23_00_55_378	nc_173	continuu
fms_2020_01_19_22_32_58_982	nc_173	continuu
fms_2020_01_19_22_25_53_240	nc_173	continuu
fms_2020_01_19_18_42_34_343	nc_173	continuu
fms_2020_01_19_13_48_00_83	nc_173	continuu

_index :"ncsearch_fms_2020_01_29_20_55_00_837"

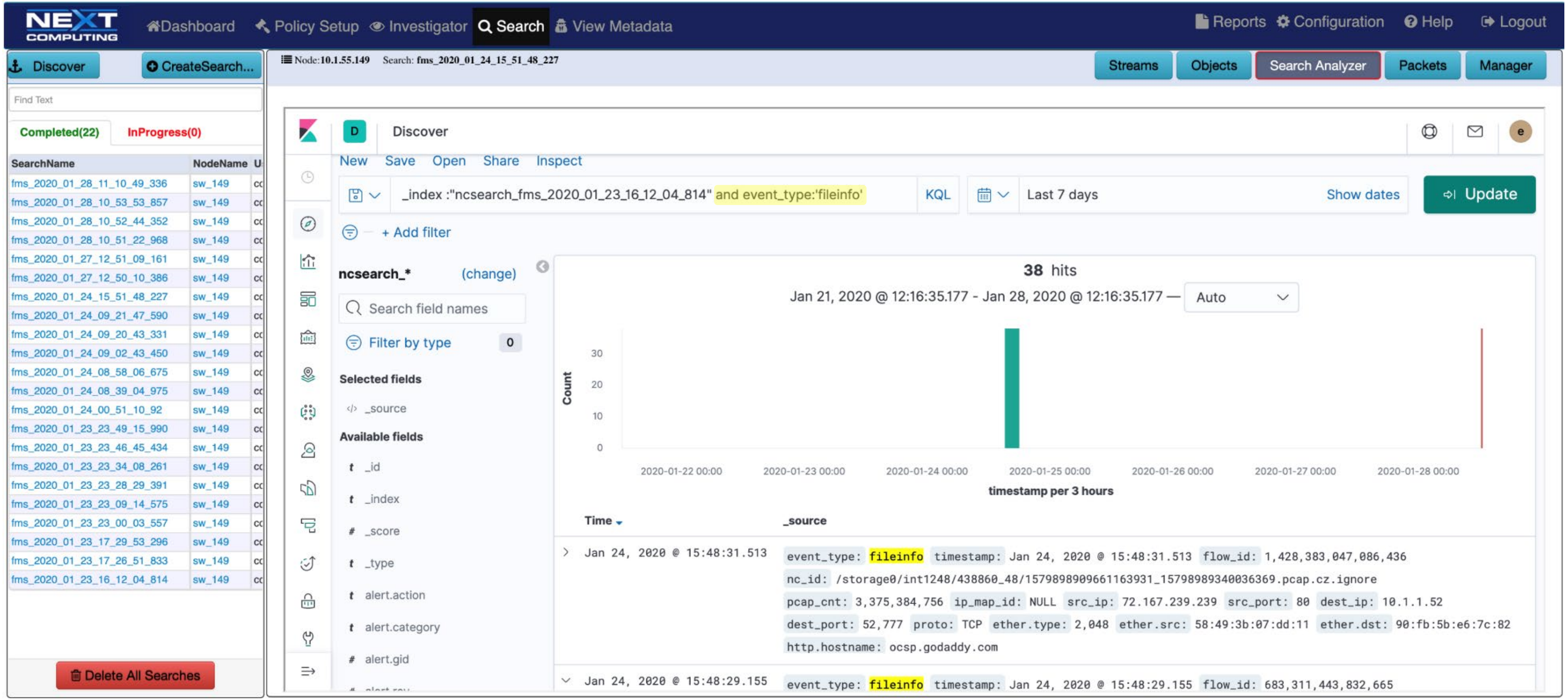
4,981 hits

Jan 22, 2020 @ 21:00:38.235 - Jan 29, 2020 @ 21:00:38.235 —

```
Time          _source
> Jan 29, 2020 @ 20:51:58.125   timestamp: Jan 29, 2020 @ 20:51:58.125 flow_id: 441,431,213,717,392 nc_id: /storage0/int111/438985_51/1580349117352877224_1580349118008308.pcap.cz.ignore
  pcap_cnt: 1,009,083,509 event_type: fileinfo ip_map_id: vm virtual network src_ip: 63.245.197.112 src_port: 80 dest_ip: 192.168.15.62 dest_port: 59,366
  proto: TCP ether.type: 2,048 ether.src: 00:27:04:25:5b:44 ether.dst: f8:b1:56:a7:a4:70 http.hostname: stats.norton.com http.url: /n/p?
  module=5024&error=1&language=09.01&hits=10000&a=%7B9FC42659-123E-47A0-BC57-
  28BC933927FA%7D&b=1&c=80&d=0&e=1&f=1&g=1&j=0&k=2&n=5&p=60&v=0&w=300&x=0&y=95&z=4&s=0&u=0&product=Endpoint%20Protection.cloud&version=22.6.4.5&OS=6.1.7601.1.0.1.0
> Jan 29, 2020 @ 20:51:55.950   timestamp: Jan 29, 2020 @ 20:51:55.950 flow_id: 173,365,124,714,557 nc_id: /storage0/int111/438985_51/1580349112880633911_1580349115008294.pcap.cz.ignore
```

Search Results: Investigator View

Search Workflow - Forensics investigations based on search or pivot from an alert in Cisco Stealthwatch



Completed(22) InProgress(0)

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

Node:10.1.55.149 Search: fms_2020_01_24_15_51_48_227

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

Last 7 days

ncsearch_*

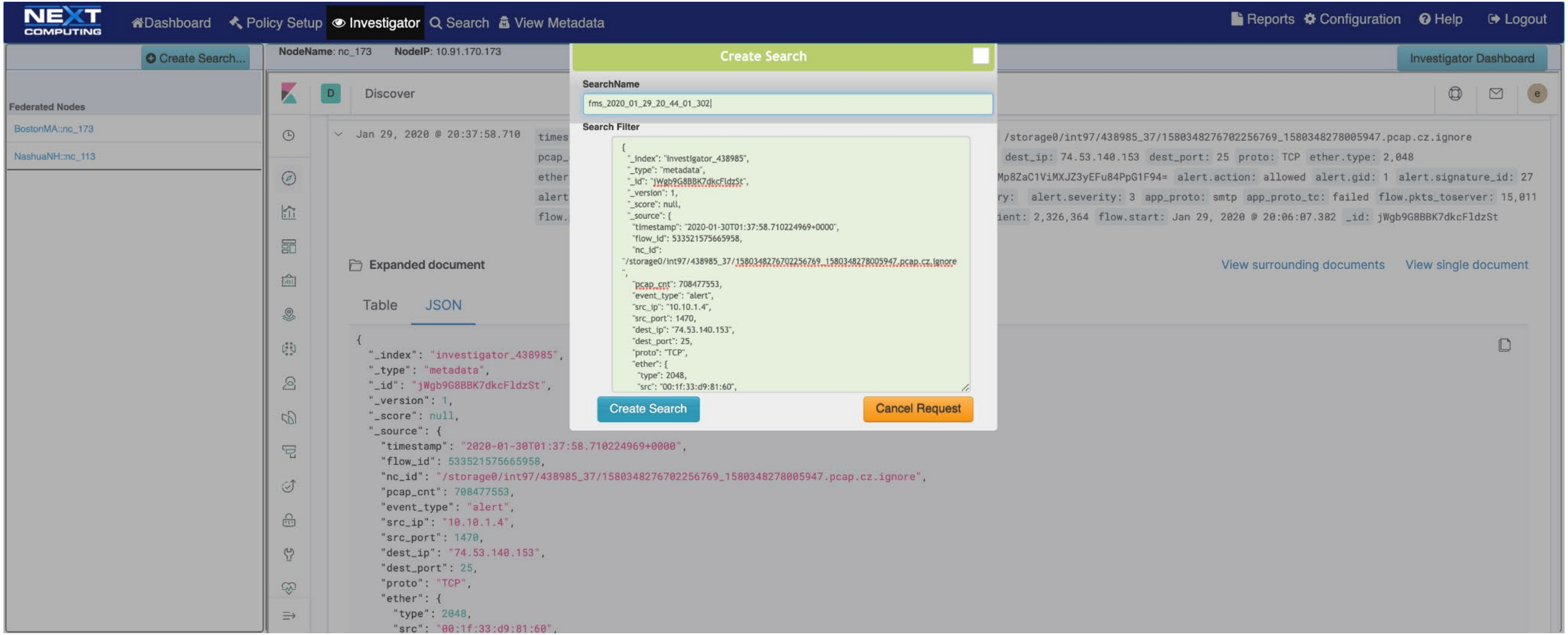
38 hits

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
```

Search Results: Investigator View, with file-type highlighted

Search Workflow - Forensics investigations based on search or pivot from an alert in Cisco Stealthwatch



NodeName: nc_173 NodeIP: 10.91.170.173

Federated Nodes

BostonMA::nc_173

NashuaNH::nc_113

```
Jan 29, 2020 @ 20:37:58.710   times                  /storage0/int97/438985_37/1580348276702256769_1580348278005947.pcap.cz.ignore
                              pcap_                  dest_ip: 74.53.140.153 dest_port: 25 proto: TCP ether.type: 2,048
                              ether                 Mp8ZaC1ViMXJZ3yEFu84PpG1F94= alert.action: allowed alert.gid: 1 alert.signature_id: 27
                              alert                 ry:  alert.severity: 3 app_proto: smtp app_proto_tc: failed flow.pkts_toserver: 15,011
                              flow.                 ient: 2,326,364 flow.start: Jan 29, 2020 @ 20:06:07.382 _id: jWgb9G8BBK7dkcFldzSt
```

```
{
  "_index": "investigator_438985",
  "_type": "metadata",
  "_id": "jWgb9G8BBK7dkcFldzSt",
  "_version": 1,
  "_score": null,
  "_source": {
    "timestamp": "2020-01-30T01:37:58.710224969+0000",
    "flow_id": 533521575665958,
    "nc_id": "/storage0/int97/438985_37/1580348276702256769_1580348278005947.pcap.cz.ignore",
    "pcap_cnt": 708477553,
    "event_type": "alert",
    "src_ip": "10.10.1.4",
    "src_port": 1470,
    "dest_ip": "74.53.140.153",
    "dest_port": 25,
    "proto": "TCP",
    "ether": {
      "type": 2048,
      "src": "00:1f:33:d9:81:60",
```

Create Search

SearchName

fms_2020_01_29_20_44_01_302

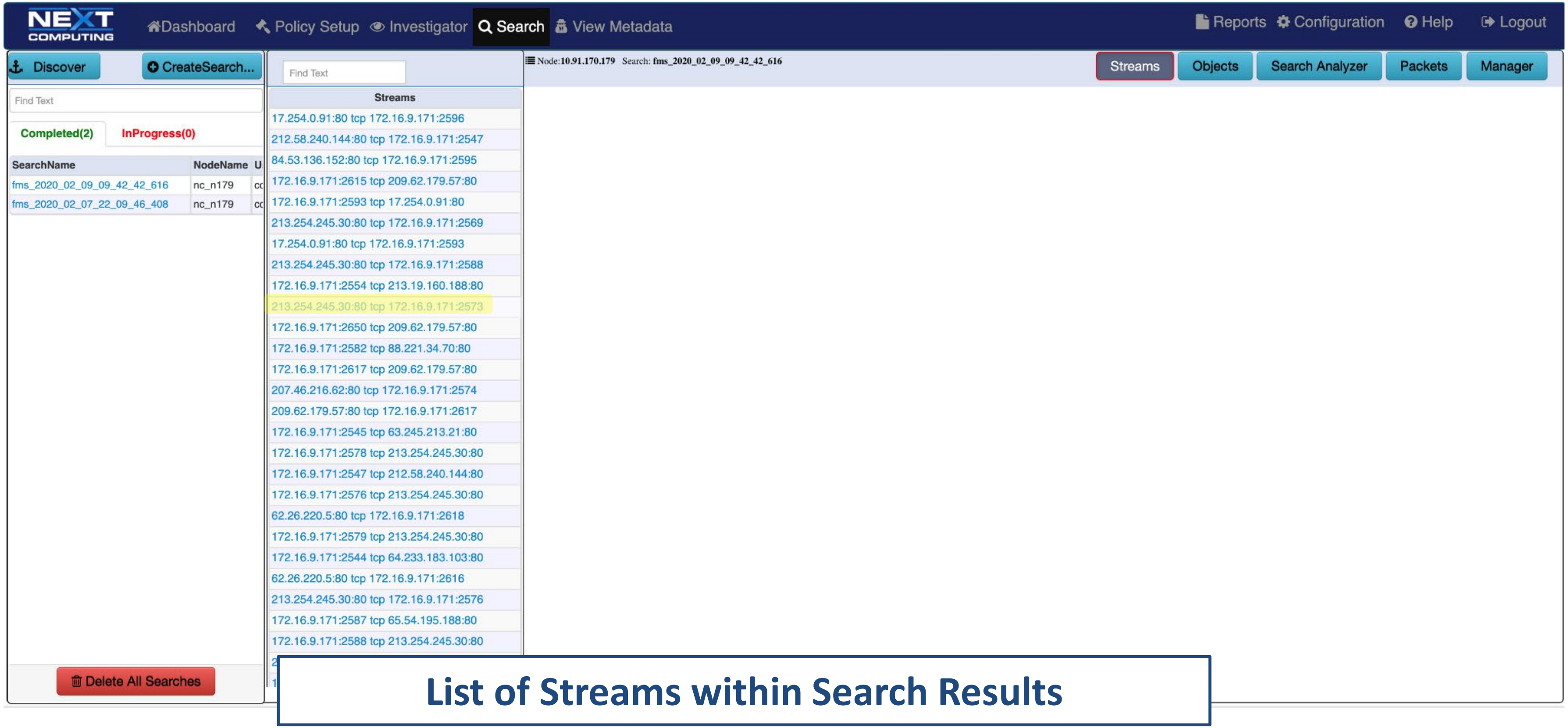
Search Filter

```
{
  "_index": "investigator_438985",
  "_type": "metadata",
  "_id": "jWgb9G8BBK7dkcFldzSt",
  "_version": 1,
  "_score": null,
  "_source": {
    "timestamp": "2020-01-30T01:37:58.710224969+0000",
    "flow_id": 533521575665958,
    "nc_id":
"/storage0/int97/438985_37/1580348276702256769_1580348278005947.pcap.cz.ignore
",
    "pcap_cnt": 708477553,
    "event_type": "alert",
    "src_ip": "10.10.1.4",
    "src_port": 1470,
    "dest_ip": "74.53.140.153",
    "dest_port": 25,
    "proto": "TCP",
    "ether": {
      "type": 2048,
      "src": "00:1f:33:d9:81:60",
```

Create Search | Cancel Request

Iterate a new Search – directly from the Investigator

Follow the Stream Workflow - for a Forensics Investigation based on search results with streams



Node:10.91.170.179 Search: fms_2020_02_09_09_42_42_616

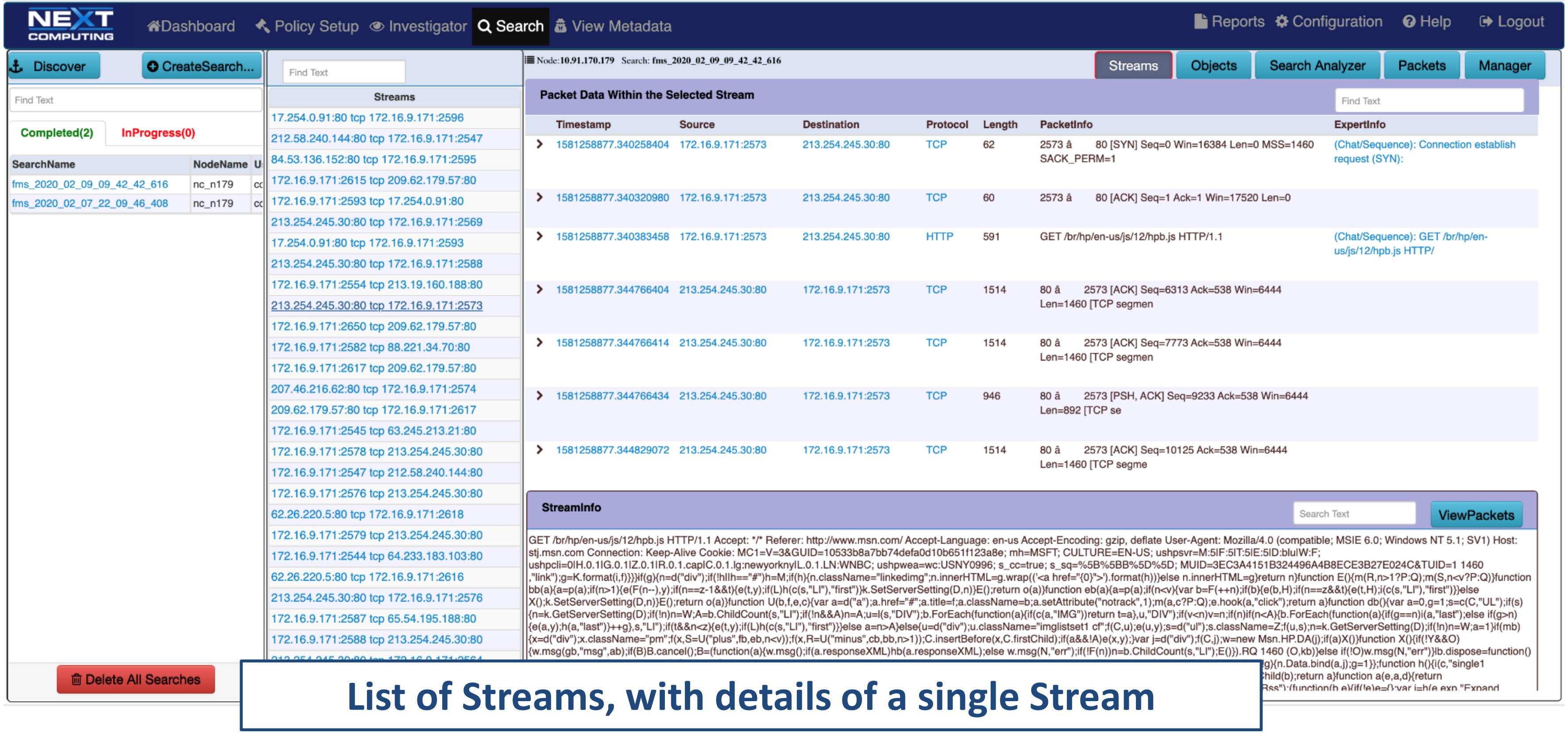
SearchName	NodeName	U
fms_2020_02_09_09_42_42_616	nc_n179	cc
fms_2020_02_07_22_09_46_408	nc_n179	cc

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

List of Streams within Search Results

www.packetcontinuum.com

Follow the Stream Workflow - for a Forensics Investigation based on search results with streams



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

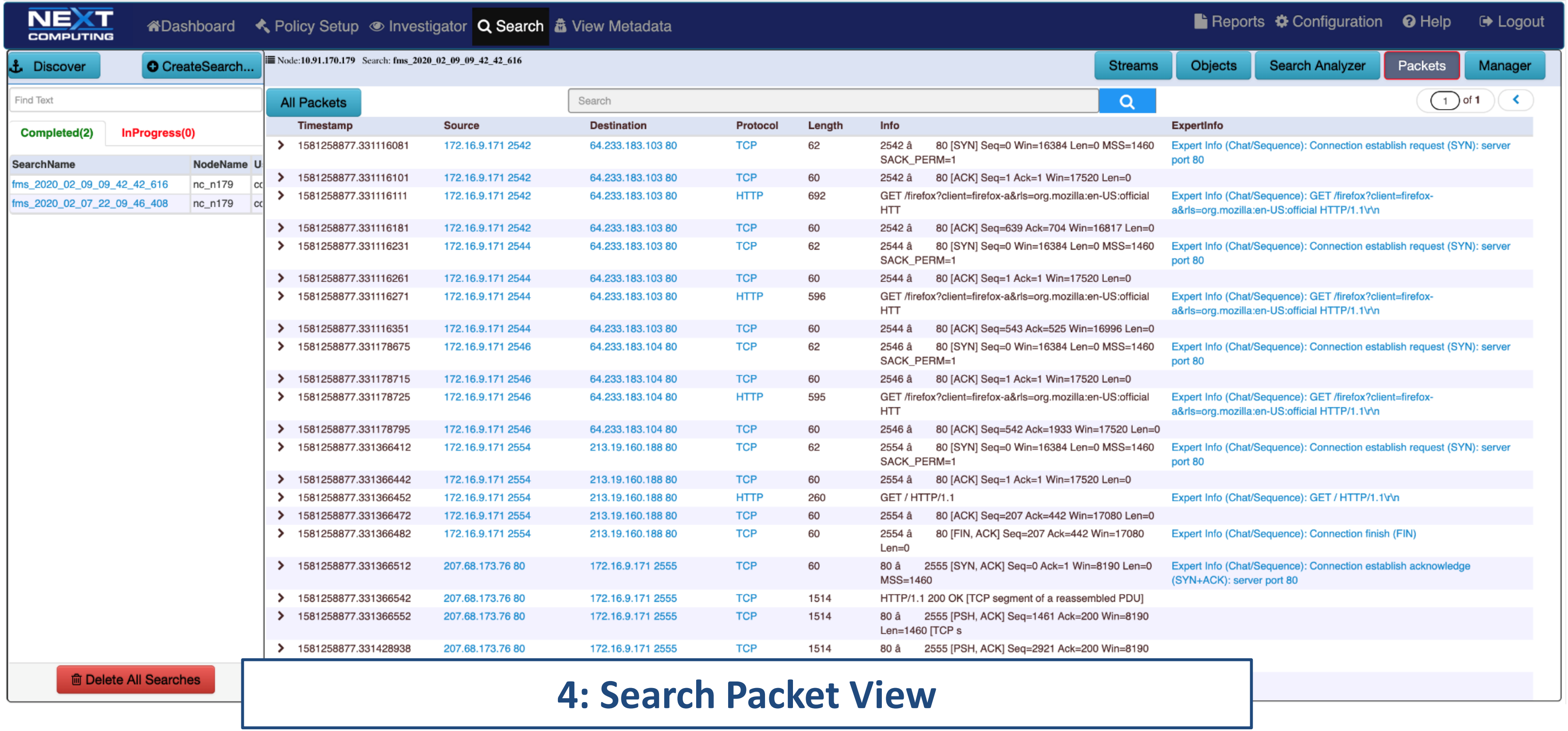
	Timestamp	Source	Destination	Protocol	Length	PacketInfo	ExpertInfo
›	1581258877.340258404	172.16.9.171:2573	213.254.245.30:80	TCP	62	2573 â 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1	(Chat/Sequence): Connection establish request (SYN):
›	1581258877.340320980	172.16.9.171:2573	213.254.245.30:80	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:blulW:F;
ushpcli=0IH.0.1IG.0.1IZ.0.1IR.0.1.capIC.0.1.lg:newyorknylL.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(!hIIh=="#")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()
g){n.Data.bind(a,j);g=1}};function h(){i(c,"single1
hild(b);return a}function a(e,a,d){return
Rss"):(function(b,e){if(!e)e=0;var i=h(e,exp,"Expand
```

List of Streams, with details of a single Stream

Follow the Stream Workflow - for a Forensics Investigation based on search results with streams



Completed(2) InProgress(0)

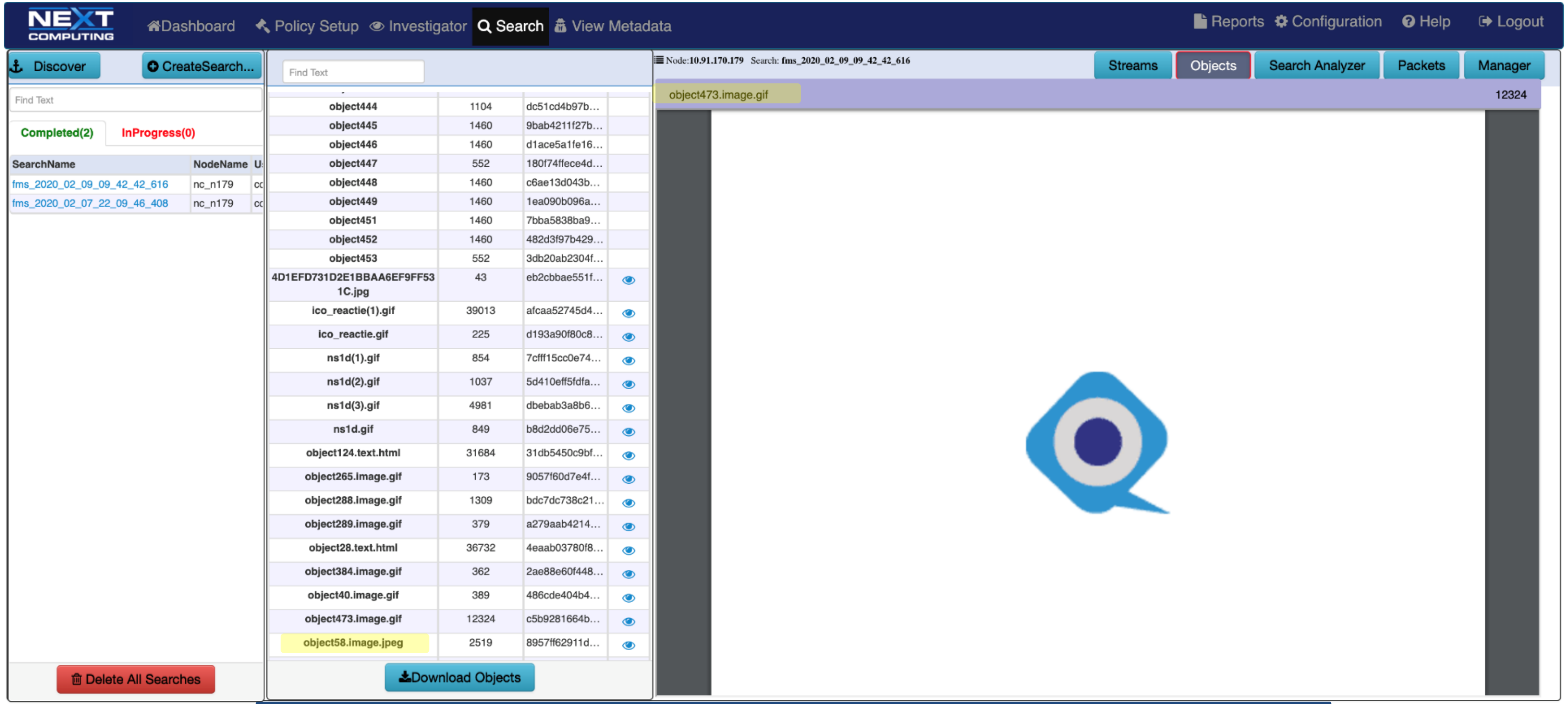
SearchName	NodeName	U
fms_2020_02_09_09_42_42_616	nc_n179	cc
fms_2020_02_07_22_09_46_408	nc_n179	cc

Node:10.91.170.179 Search: fms_2020_02_09_09_42_42_616

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	

4: Search Packet View

Follow the Stream Workflow - for a Forensics Investigation based on search results with streams



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

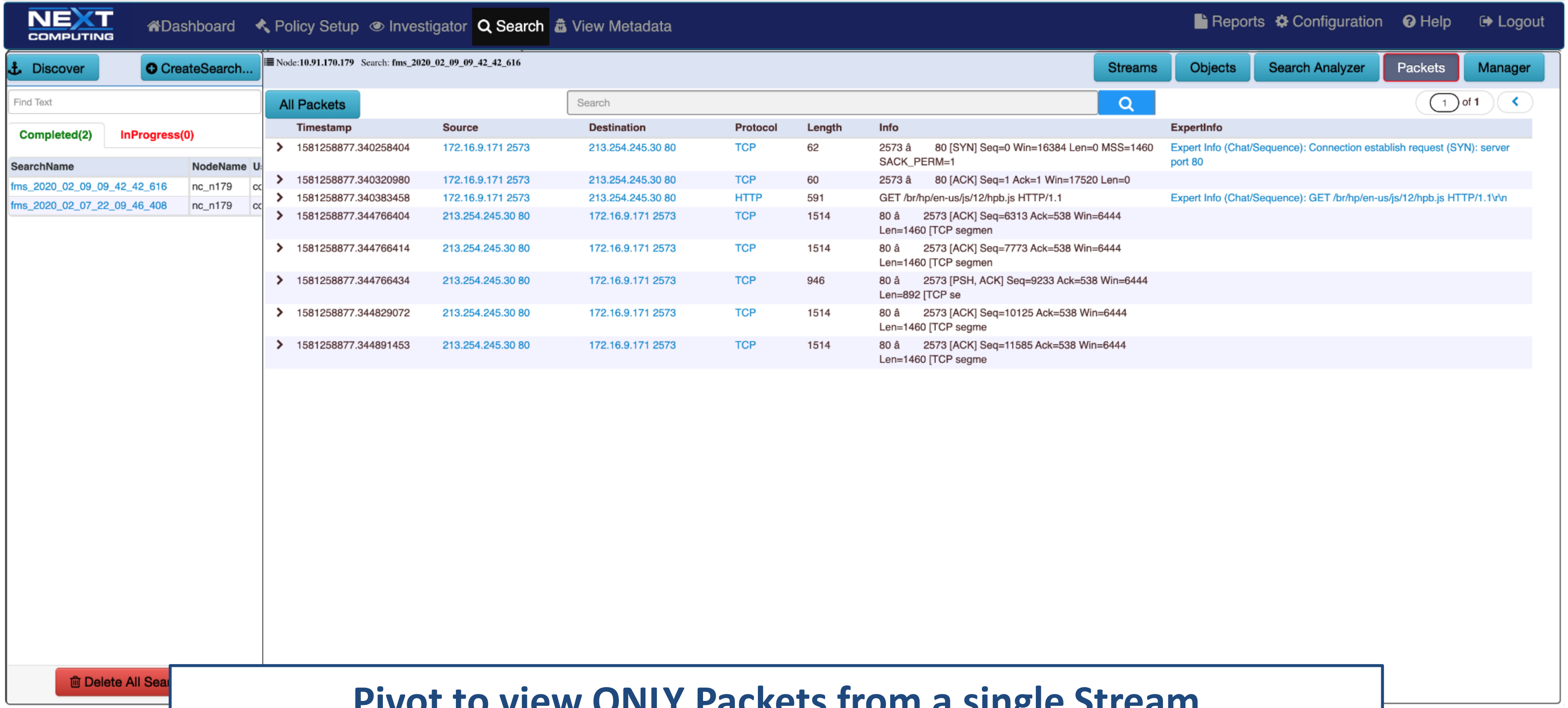
object444	1104	dc51cd4b97b...	
object445	1460	9bab4211f27b...	
object446	1460	d1ace5a1fe16...	
object447	552	180f74ffece4d...	
object448	1460	c6ae13d043b...	
object449	1460	1ea090b096a...	
object451	1460	7bba5838ba9...	
object452	1460	482d3f97b429...	
object453	552	3db20ab2304f...	
4D1EFD731D2E1BBAA6EF9FF531C.jpg	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

5: List of Objects of a Search, plus a single Object View

Follow the Stream Workflow - for a Forensics Investigation based on search results with streams



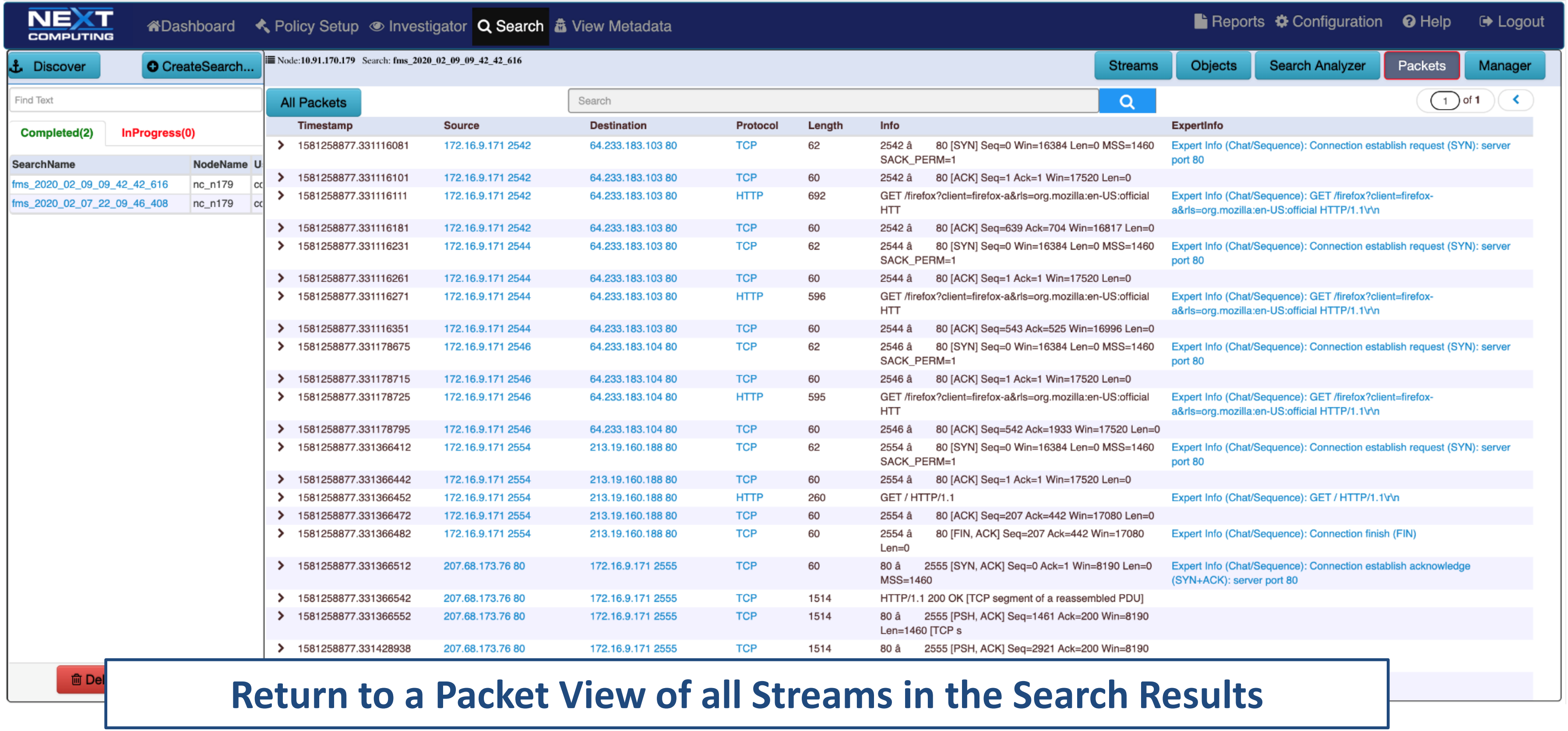
Node:10.91.170.179 Search: fms_2020_02_09_09_42_42_616

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
1581258877.340258404	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	Expert Info (Chat/Sequence): Connection establish request (SYN): server port 80
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	Expert Info (Chat/Sequence): GET /br/hp/en-us/js/12/hpb.js HTTP/1.1\r\n
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	
1581258877.344891453	213.254.245.30 80	172.16.9.171 2573	TCP	1514	80 â 2573 [ACK] Seq=11585 Ack=538 Win=6444 Len=1460 [TCP segme	

Pivot to view ONLY Packets from a single Stream

Follow the Stream Workflow - for a Forensics Investigation based on search results with streams



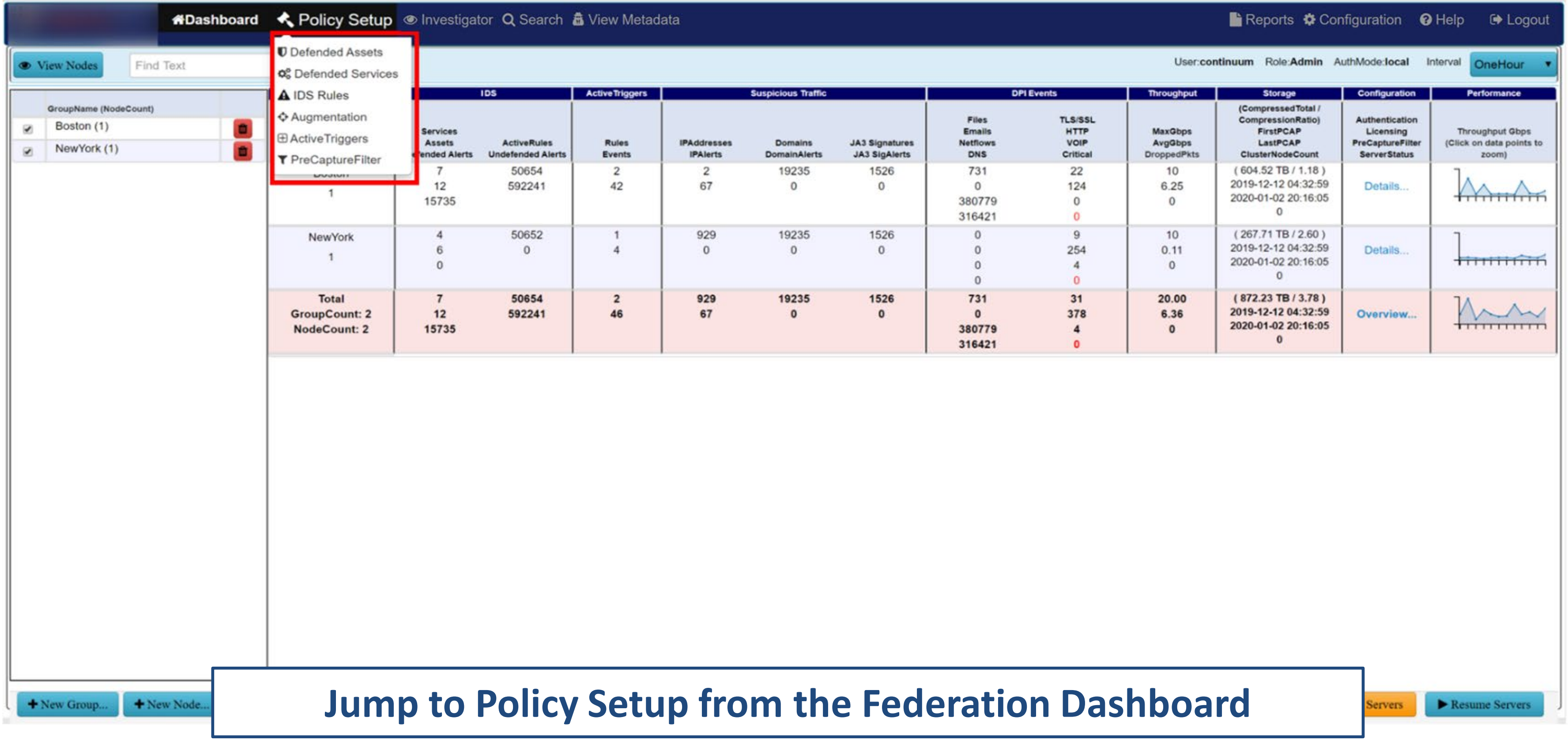
Completed(2) InProgress(0)

SearchName	NodeName	U
fms_2020_02_09_09_42_42_616	nc_n179	co
fms_2020_02_07_22_09_46_408	nc_n179	co

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	

Return to a Packet View of all Streams in the Search Results

Policy Update Workflow – Quickly change real-time policies, based on new threat intel or lessons-learned. Federation Manager will PUSH policies to ALL field appliances.



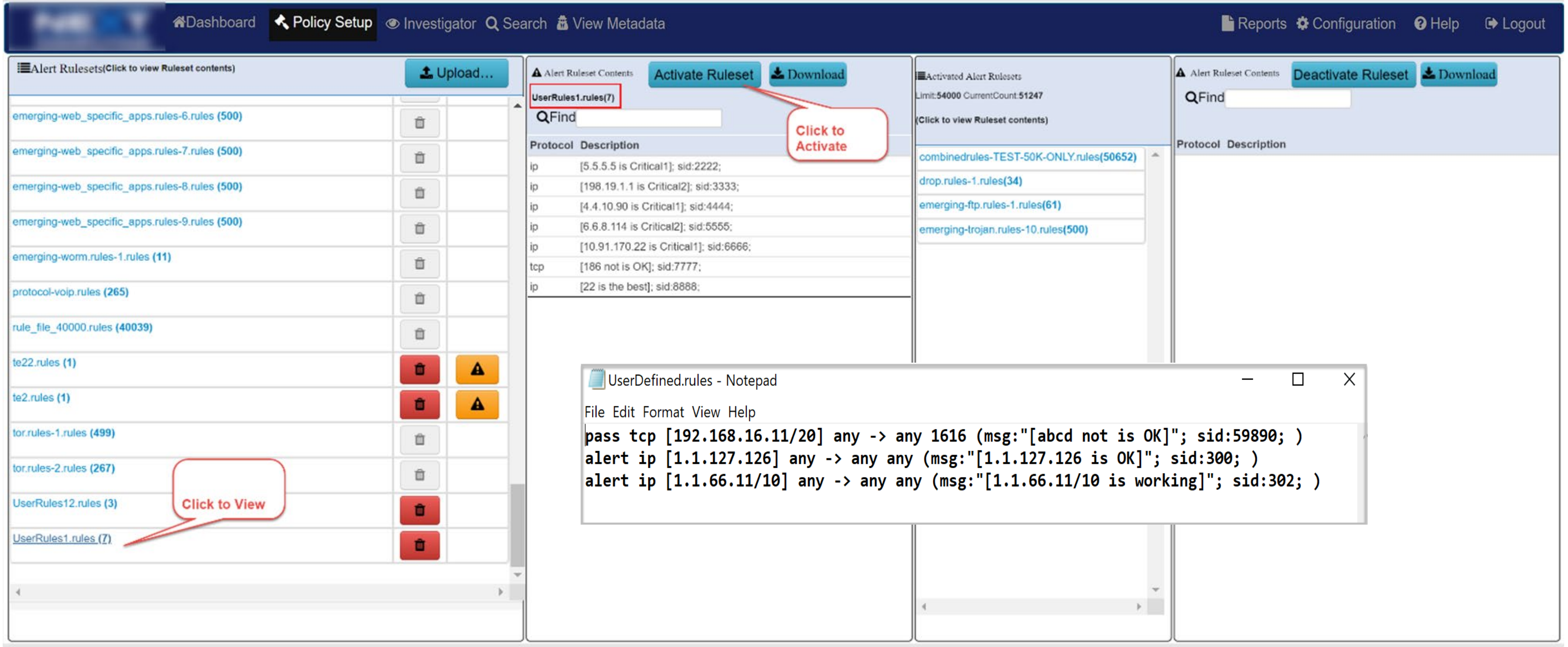
User:continuum Role:Admin AuthMode:local Interval OneHour

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

	IDS		ActiveTriggers	Suspicious Traffic			DPI Events		Throughput	Storage	Configuration	Performance
	Services Assets fended 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

Policy Update Workflow – Quickly change real-time policies, based on new threat intel or lessons-learned. Federation Manager will PUSH policies to ALL field appliances.



Alert Rulesets(Click to view Ruleset contents)

- emerging-web_specific_apps.rules-6.rules (500)
- emerging-web_specific_apps.rules-7.rules (500)
- emerging-web_specific_apps.rules-8.rules (500)
- emerging-web_specific_apps.rules-9.rules (500)
- emerging-worm.rules-1.rules (11)
- protocol-voip.rules (265)
- rule_file_40000.rules (40039)
- te22.rules (1)
- te2.rules (1)
- tor.rules-1.rules (499)
- tor.rules-2.rules (267)
- UserRules12.rules (3)
- UserRules1.rules (7)

Click to View

Alert Ruleset Contents

UserRules1.rules(7)

Protocol	Description
ip	[5.5.5.5 is Critical1]; sid:2222;
ip	[198.19.1.1 is Critical2]; sid:3333;
ip	[4.4.10.90 is Critical1]; sid:4444;
ip	[6.6.8.114 is Critical2]; sid:5555;
ip	[10.91.170.22 is Critical1]; sid:6666;
tcp	[186 not is OK]; sid:7777;
ip	[22 is the best]; sid:8888;

Click to Activate

Activated Alert Rulesets

Limit:54000 CurrentCount:51247

(Click to view Ruleset contents)

- combinedrules-TEST-50K-ONLY.rules(50652)
- drop.rules-1.rules(34)
- emerging-ftp.rules-1.rules(61)
- emerging-trojan.rules-10.rules(500)

Alert Ruleset Contents

Protocol	Description

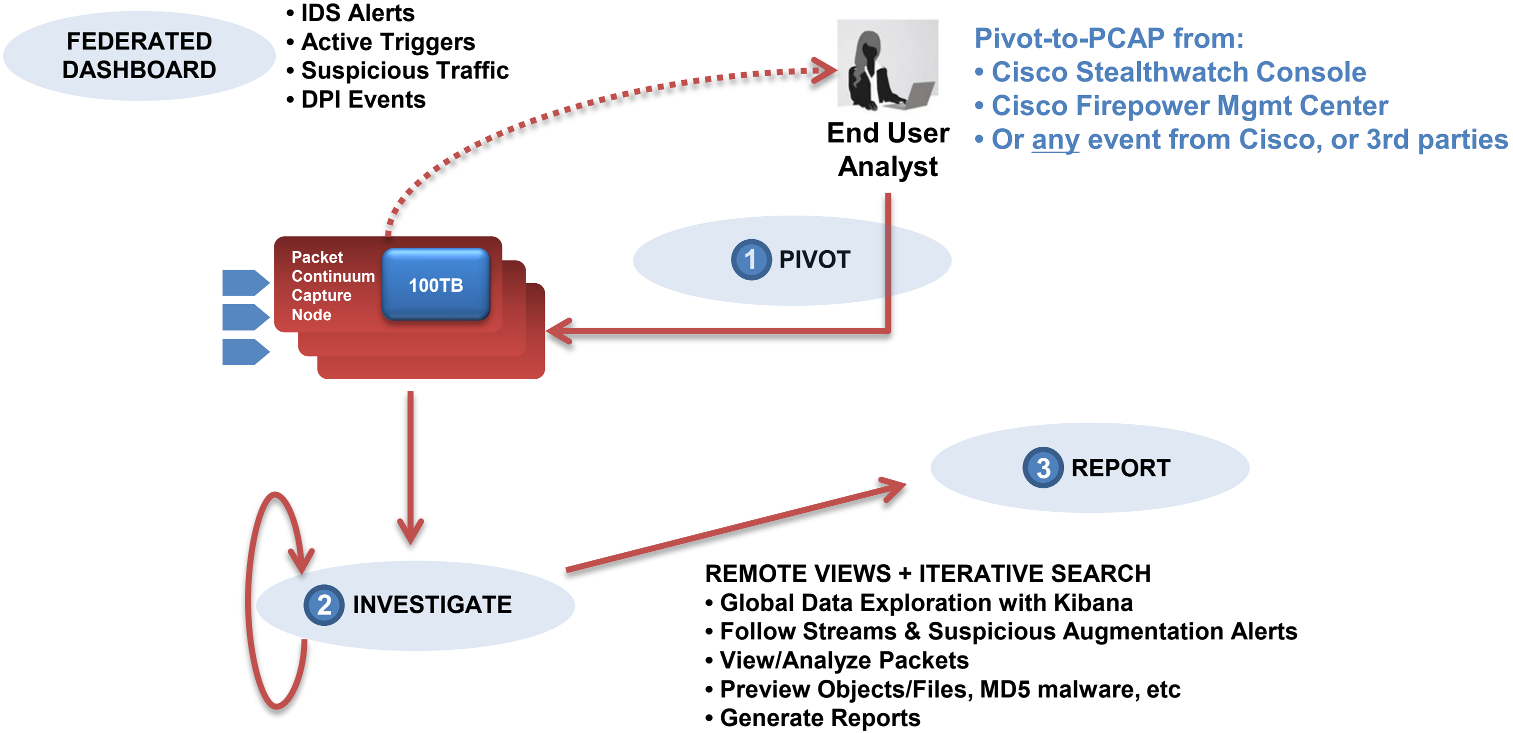
UserDefined.rules - Notepad

File Edit Format View Help

```
pass tcp [192.168.16.11/20] any -> any 1616 (msg:"[abcd not is OK]"; sid:59890; )
alert ip [1.1.127.126] any -> any any (msg:"[1.1.127.126 is OK]"; sid:300; )
alert ip [1.1.66.11/10] any -> any any (msg:"[1.1.66.11/10 is working]"; sid:302; )
```

Select IDS rulesets from pre-loaded libraries, or create user-defined rules

Simplified PCAP Workflow: Summary



FEDERATED DASHBOARD

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

End User Analyst

Pivot-to-PCAP from:

- Cisco Stealthwatch Console
- Cisco Firepower Mgmt Center
- Or any 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

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