EndaceProbe Analytics Platform and Cisco Stealthwatch

Cisco Stealthwatch

Together, Endace and Cisco Stealthwatch outsmart emerging threats with scalable visibility and security analytics complemented by 100% accurate network packet capture. Dive deep into anomalous network activity and security events for rapid and conclusive investigations.

Cisco Stealthwatch is a comprehensive, network telemetry-based, security monitoring and analytics solution that streamlines incident response through behavioral analysis; detecting denial of service attacks, anomalous behaviour, malicious activity and insider threats. Based on a scalable enterprise architecture, Stealthwatch provides near real-time situational awareness of all users and devices on the network.

The EndaceProbe™ Analytics Platform captures and records 100% of network traffic, regardless of network speeds or loads, providing an unparalleled level of detail and accuracy. Recorded network packets are time-stamped to nanosecond-level accuracy allowing analysts to zoom in to investigate short-lived events, such as microbursts or pre-attack intrusions, that are often invisible to other monitoring solutions. Access to detailed packet-level history lets analysts accurately reconstruct events to identify conclusively what happened, why and how it happened and to then respond appropriately. Critical issues can be prioritized, and false positives quickly identified and flagged so detection can be tuned.

EndaceProbes complement Stealthwatch by capturing, recording and indexing all traffic on the network down to the nanosecond level. Access to historical network traffic provides context and deterministic root cause for security events flagged by Stealthwatch. Using the External Lookup feature in the Stealthwatch Management Console (SMC), analysts can seamlessly pivot from an event in SMC to the associated packet data on EndaceProbes on the network.

Deploying Stealthwatch Flow Sensor Virtual Edition on EndaceProbe can produce telemetry for segments of the switching and routing infrastructure that can't generate NetFlow natively and provides visibility into application layer data. It can also help remove flow generation load from critical infrastructural elements such as key routers and switches.

PRODUCTS

Cisco Stealthwatch

EndaceProbe Analytics Platform Endace Fusion Stealthwatch Connector

BENEFITS

- Scalable security management for your networked environment.
- Accurate, complete and granular network history provides definitive evidence for investigating and responding to network security and performance issues.
- Streamlined investigation workflow improves SecOps and NetOps efficiency and ensures rapid investigation and response.
- Faster resolution times increase network security, improve uptime and reliability and reduce OPEX costs
- Recorded network history provides a reliable, irrefutable evidence trail for comprehensive investigations.

FURTHER INFORMATION

www.endace.com/cisco_stealthwatch.html

Streamlining Security Investigations

Endace's Fusion Connector for Stealthwatch is a free, easy to install plugin available from the Endace Support Portal. It directly connects analysts, via an elegant and seamless workflow, to the precise network packets they need to investigate the root cause of problems and respond.

Analysts can click on any event triggered to pivot straight to the packets of interest in EndaceVision, the EndaceProbe's built-in, browser-based investigation tool. With the relevant packets isolated in EndaceVision, analysts can zoom out to look at precursor events, or zoom in to look at packet-level detail in EndacePackets, the EndaceProbe's integrated packet decode tool.

Alternatively, Stealthwatch users can download PCAP or ERF files directly to their desktop where they can be analyzed using Wireshark® or other packet decode tools.

Increasing Stealthwatch Visibility and Coverage

Stealthwatch Flow Sensor VE can be hosted in the EndaceProbe's Application Dock™ built-in hosting environment where every packet captured and recorded by the EndaceProbe can also be streamed to hosted Flow Sensor instances in real-time.

Security Operations teams can dynamically deploy Flow Sensors anywhere on the network that they have EndaceProbe Network Recorders deployed, allowing them to increase visibility without truck rolls or lengthy hardware deployments.

EndaceProbes are designed to ensure system resources used for capture and recording are separated from the resources used by hosted applications. This means capture performance is never impacted by hosted applications and vice-versa, guaranteeing 100% accurate recording even when the hosted Flow Sensor instance is processing heavy traffic loads.

Conclusion

Integrating captured network packet history from EndaceProbes with Cisco Stealthwatch Enterprise speeds up incident response and forensics. The efficient workflow integration gives security teams a way to quickly and conclusively investigate and respond to security issues that Stealthwatch detects.

It provides a standardized, streamlined investigation workflow that allows analysts to quickly identify the scale and root cause of an issue and respond appropriately to minimize the damage.

Deploying Stealthwatch Flow Sensors on EndaceProbe hardware allows customers to extend visibility to the far reaches of the network. Customers can remove flow generation overhead from their core network elements such as routers and switches, ensuring that critical monitoring data will still be generated even when the network is heavily loaded or there is a fault in the network infrastructure.

How it works

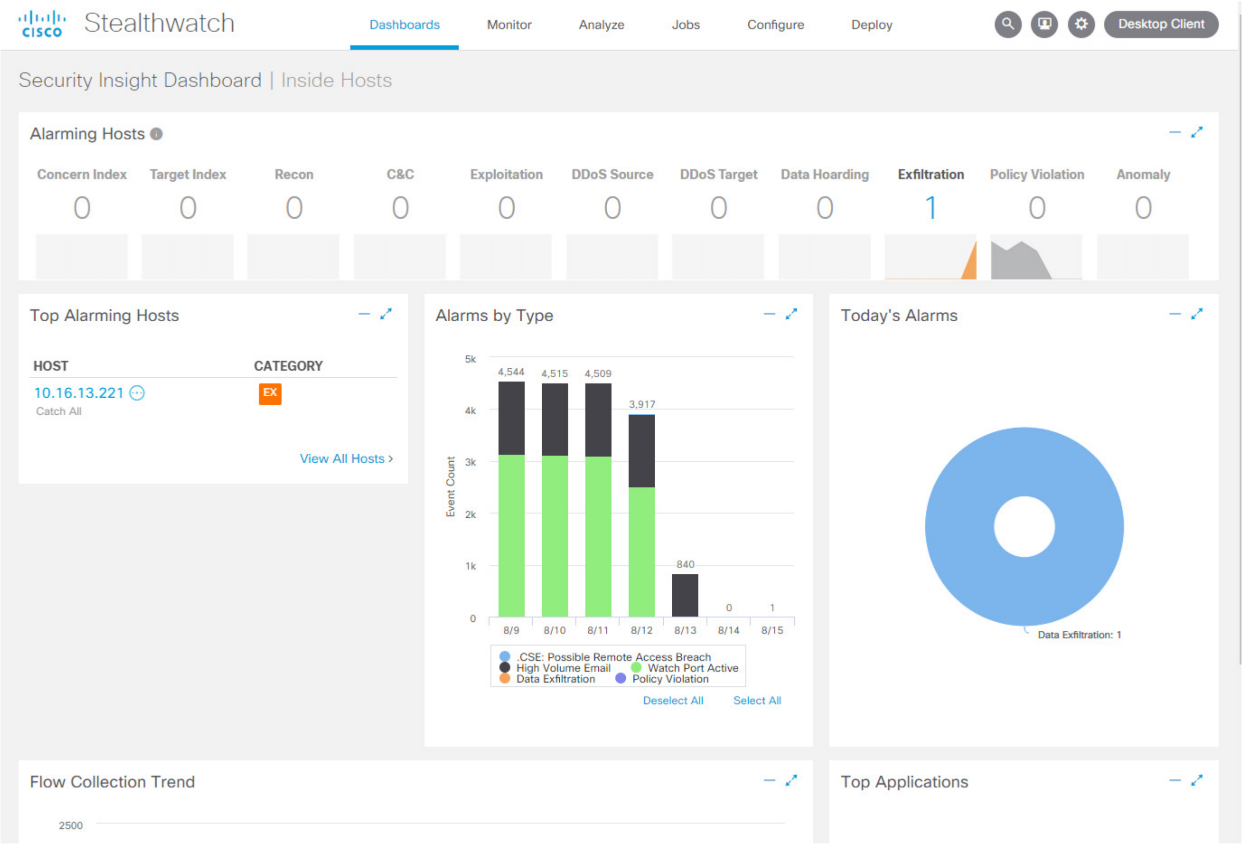
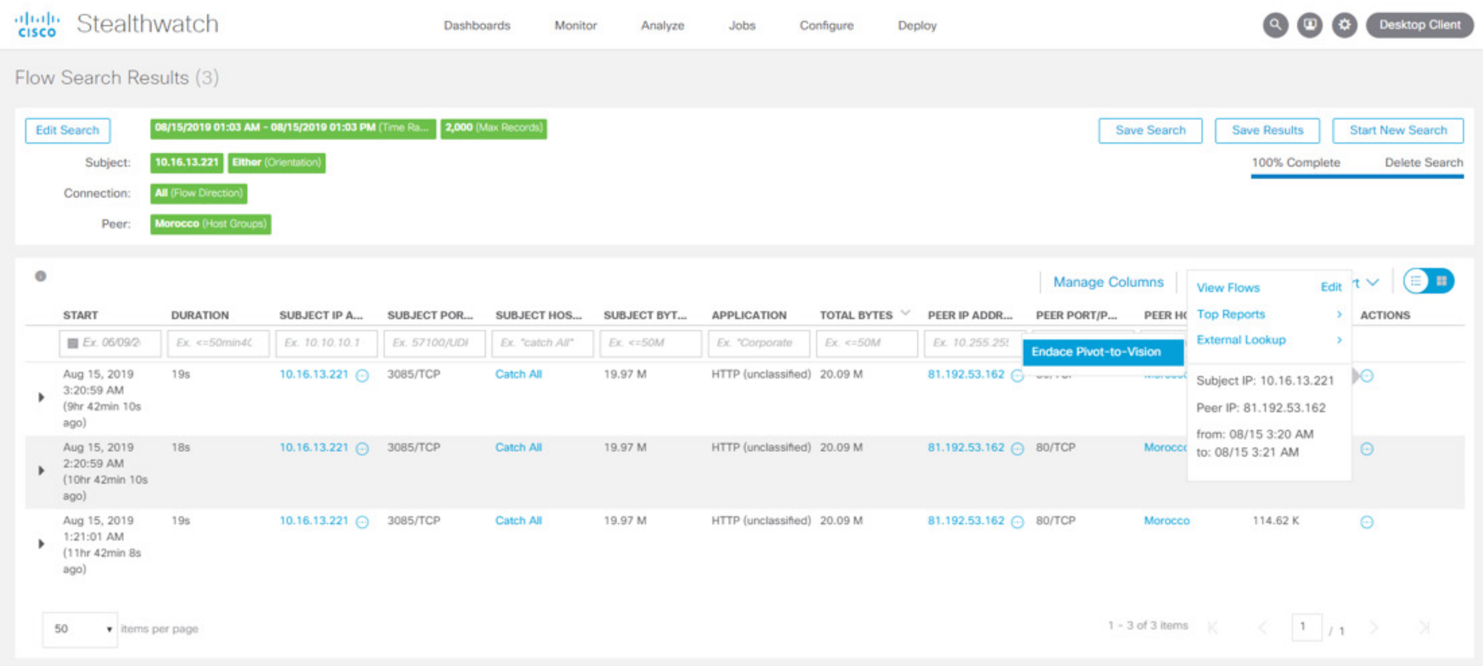


Figure 1. Triage your security alarms with the Stealthwatch Dashboard



Flow Search Results (3)

08/15/2019 01:03 AM - 08/15/2019 01:03 PM (Time Ra... 2,000 (Max Records)

Subject: 10.16.13.221 Either (Orientation)

Connection: All (Flow Direction)

Peer: Morocco (Host Groups)

100% Complete

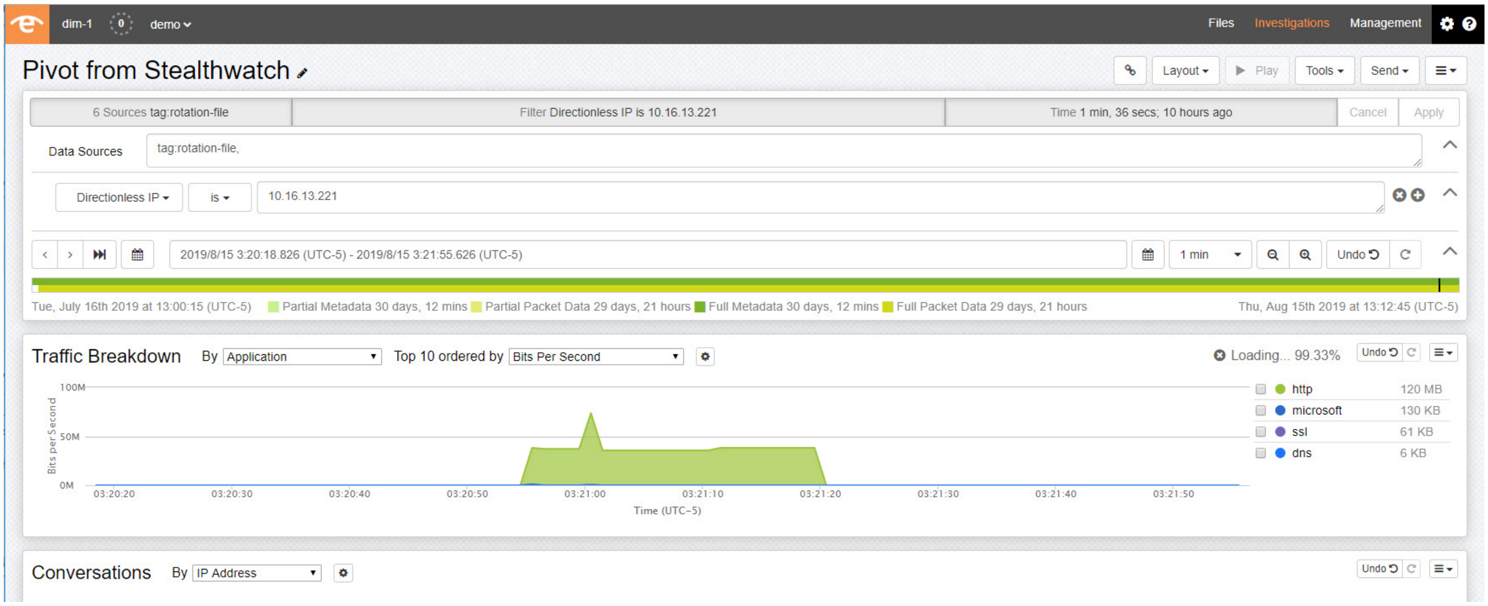
START	DURATION	SUBJECT IP A...	SUBJECT POR...	SUBJECT HOS...	SUBJECT BYT...	APPLICATION	TOTAL BYTES	PEER IP ADDR...	PEER PORT/P...	PEER HC		ACTIONS
Ex. 06/09/2	Ex. <=50min4C	Ex. 10.10.10.1	Ex. 57100/UDI	Ex. "catch All"	Ex. <=50M	Ex. "Corporate	Ex. <=50M	Ex. 10.255.25!				
Aug 15, 2019 3:20:59 AM (9hr 42min 10s ago)	19s	10.16.13.221	3085/TCP	Catch All	19.97 M	HTTP (unclassified)	20.09 M	81.192.53.162				
Aug 15, 2019 2:20:59 AM (10hr 42min 10s ago)	18s	10.16.13.221	3085/TCP	Catch All	19.97 M	HTTP (unclassified)	20.09 M	81.192.53.162	80/TCP	Morocco		
Aug 15, 2019 1:21:01 AM (11hr 42min 8s ago)	19s	10.16.13.221	3085/TCP	Catch All	19.97 M	HTTP (unclassified)	20.09 M	81.192.53.162	80/TCP	Morocco	114.62 K	

Subject IP: 10.16.13.221
Peer IP: 81.192.53.162
from: 08/15 3:20 AM
to: 08/15 3:21 AM

50 items per page

1 - 3 of 3 items 1 / 1

Figure 2. Pivot-to-Vision launches EndaceVision pre-filtered in on the packets related to the event in question.



Pivot from Stealthwatch

6 Sources tag:rotation-file | Filter Directionless IP is 10.16.13.221 | Time 1 min, 36 secs; 10 hours ago

Data Sources: tag:rotation-file,

Directionless IP is 10.16.13.221

2019/8/15 3:20:18.826 (UTC-5) - 2019/8/15 3:21:55.626 (UTC-5) 1 min

Tue, July 16th 2019 at 13:00:15 (UTC-5) Partial Metadata 30 days, 12 mins Partial Packet Data 29 days, 21 hours Full Metadata 30 days, 12 mins Full Packet Data 29 days, 21 hours Thu, Aug 15th 2019 at 13:12:45 (UTC-5)

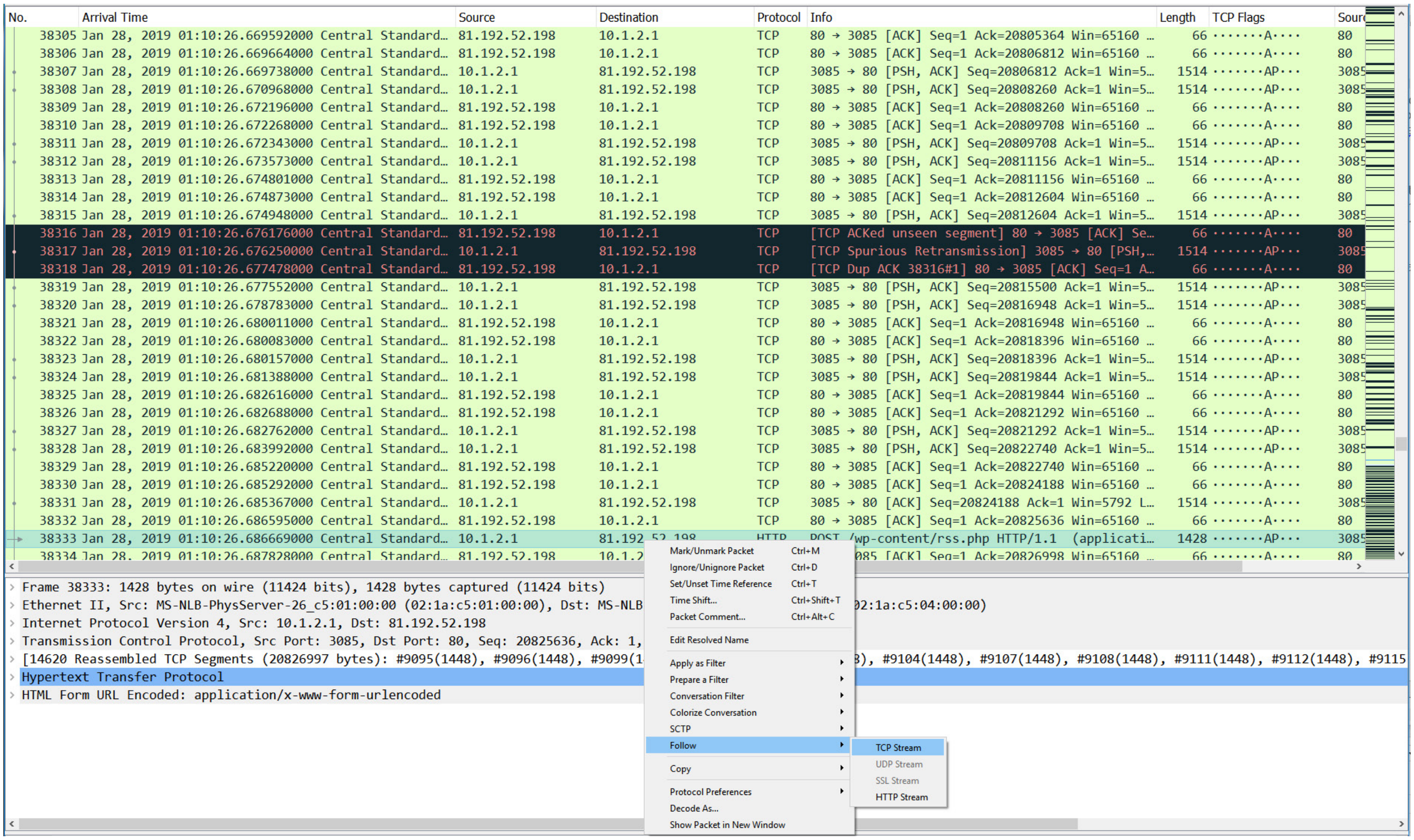
Traffic Breakdown By Application Top 10 ordered by Bits Per Second

Loading... 99.33%

http	120 MB
microsoft	130 KB
ssl	61 KB
dns	6 KB

Conversations By IP Address

Figure 3. Analyze network history with EndaceVision - a powerful, browser based traffic analysis tool.



```
No.   Arrival Time                                 Source         Destination    Protocol Info                                                Length TCP Flags      Sourc
 38305 Jan 28, 2019 01:10:26.669592000 Central Standard… 81.192.52.198  10.1.2.1       TCP  80 → 3085 [ACK] Seq=1 Ack=20805364 Win=65160 …          66 ·······A····  80
 38306 Jan 28, 2019 01:10:26.669664000 Central Standard… 81.192.52.198  10.1.2.1       TCP  80 → 3085 [ACK] Seq=1 Ack=20806812 Win=65160 …          66 ·······A····  80
 38307 Jan 28, 2019 01:10:26.669738000 Central Standard… 10.1.2.1       81.192.52.198  TCP  3085 → 80 [PSH, ACK] Seq=20806812 Ack=1 Win=5…        1514 ·······AP···  3085
 38308 Jan 28, 2019 01:10:26.670968000 Central Standard… 10.1.2.1       81.192.52.198  TCP  3085 → 80 [PSH, ACK] Seq=20808260 Ack=1 Win=5…        1514 ·······AP···  3085
 38309 Jan 28, 2019 01:10:26.672196000 Central Standard… 81.192.52.198  10.1.2.1       TCP  80 → 3085 [ACK] Seq=1 Ack=20808260 Win=65160 …          66 ·······A····  80
 38310 Jan 28, 2019 01:10:26.672268000 Central Standard… 81.192.52.198  10.1.2.1       TCP  80 → 3085 [ACK] Seq=1 Ack=20809708 Win=65160 …          66 ·······A····  80
 38311 Jan 28, 2019 01:10:26.672343000 Central Standard… 10.1.2.1       81.192.52.198  TCP  3085 → 80 [PSH, ACK] Seq=20809708 Ack=1 Win=5…        1514 ·······AP···  3085
 38312 Jan 28, 2019 01:10:26.673573000 Central Standard… 10.1.2.1       81.192.52.198  TCP  3085 → 80 [PSH, ACK] Seq=20811156 Ack=1 Win=5…        1514 ·······AP···  3085
 38313 Jan 28, 2019 01:10:26.674801000 Central Standard… 81.192.52.198  10.1.2.1       TCP  80 → 3085 [ACK] Seq=1 Ack=20811156 Win=65160 …          66 ·······A····  80
 38314 Jan 28, 2019 01:10:26.674873000 Central Standard… 81.192.52.198  10.1.2.1       TCP  80 → 3085 [ACK] Seq=1 Ack=20812604 Win=65160 …          66 ·······A····  80
 38315 Jan 28, 2019 01:10:26.674948000 Central Standard… 10.1.2.1       81.192.52.198  TCP  3085 → 80 [PSH, ACK] Seq=20812604 Ack=1 Win=5…        1514 ·······AP···  3085
 38316 Jan 28, 2019 01:10:26.676176000 Central Standard… 81.192.52.198  10.1.2.1       TCP  [TCP ACKed unseen segment] 80 → 3085 [ACK] Se…     66 ·······A····  80
 38317 Jan 28, 2019 01:10:26.676250000 Central Standard… 10.1.2.1       81.192.52.198  TCP  [TCP Spurious Retransmission] 3085 → 80 [PSH,…   1514 ·······AP···  3085
 38318 Jan 28, 2019 01:10:26.677478000 Central Standard… 81.192.52.198  10.1.2.1       TCP  [TCP Dup ACK 38316#1] 80 → 3085 [ACK] Seq=1 A…     66 ·······A····  80
 38319 Jan 28, 2019 01:10:26.677552000 Central Standard… 10.1.2.1       81.192.52.198  TCP  3085 → 80 [PSH, ACK] Seq=20815500 Ack=1 Win=5…        1514 ·······AP···  3085
 38320 Jan 28, 2019 01:10:26.678783000 Central Standard… 10.1.2.1       81.192.52.198  TCP  3085 → 80 [PSH, ACK] Seq=20816948 Ack=1 Win=5…        1514 ·······AP···  3085
 38321 Jan 28, 2019 01:10:26.680011000 Central Standard… 81.192.52.198  10.1.2.1       TCP  80 → 3085 [ACK] Seq=1 Ack=20816948 Win=65160 …          66 ·······A····  80
 38322 Jan 28, 2019 01:10:26.680083000 Central Standard… 81.192.52.198  10.1.2.1       TCP  80 → 3085 [ACK] Seq=1 Ack=20818396 Win=65160 …          66 ·······A····  80
 38323 Jan 28, 2019 01:10:26.680157000 Central Standard… 10.1.2.1       81.192.52.198  TCP  3085 → 80 [PSH, ACK] Seq=20818396 Ack=1 Win=5…        1514 ·······AP···  3085
 38324 Jan 28, 2019 01:10:26.681388000 Central Standard… 10.1.2.1       81.192.52.198  TCP  3085 → 80 [PSH, ACK] Seq=20819844 Ack=1 Win=5…        1514 ·······AP···  3085
 38325 Jan 28, 2019 01:10:26.682616000 Central Standard… 81.192.52.198  10.1.2.1       TCP  80 → 3085 [ACK] Seq=1 Ack=20819844 Win=65160 …          66 ·······A····  80
 38326 Jan 28, 2019 01:10:26.682688000 Central Standard… 81.192.52.198  10.1.2.1       TCP  80 → 3085 [ACK] Seq=1 Ack=20821292 Win=65160 …          66 ·······A····  80
 38327 Jan 28, 2019 01:10:26.682762000 Central Standard… 10.1.2.1       81.192.52.198  TCP  3085 → 80 [PSH, ACK] Seq=20821292 Ack=1 Win=5…        1514 ·······AP···  3085
 38328 Jan 28, 2019 01:10:26.683992000 Central Standard… 10.1.2.1       81.192.52.198  TCP  3085 → 80 [PSH, ACK] Seq=20822740 Ack=1 Win=5…        1514 ·······AP···  3085
 38329 Jan 28, 2019 01:10:26.685220000 Central Standard… 81.192.52.198  10.1.2.1       TCP  80 → 3085 [ACK] Seq=1 Ack=20822740 Win=65160 …          66 ·······A····  80
 38330 Jan 28, 2019 01:10:26.685292000 Central Standard… 81.192.52.198  10.1.2.1       TCP  80 → 3085 [ACK] Seq=1 Ack=20824188 Win=65160 …          66 ·······A····  80
 38331 Jan 28, 2019 01:10:26.685367000 Central Standard… 10.1.2.1       81.192.52.198  TCP  3085 → 80 [ACK] Seq=20824188 Ack=1 Win=5792 L…        1514 ·······A····  3085
 38332 Jan 28, 2019 01:10:26.686595000 Central Standard… 81.192.52.198  10.1.2.1       TCP  80 → 3085 [ACK] Seq=1 Ack=20825636 Win=65160 …          66 ·······A····  80
 38333 Jan 28, 2019 01:10:26.686669000 Central Standard… 10.1.2.1       81.192.52.198  HTTP POST /wp-content/rss.php HTTP/1.1  (applicati…      1428 ·······AP···  3085
 38334 Jan 28, 2019 01:10:26.687828000 Central Standard… 81.192.52.198  10.1.2        085 [ACK] Seq=1 Ack=20826998 Win=65160 …            66 ·······A····  80
```

```
> Frame 38333: 1428 bytes on wire (11424 bits), 1428 bytes captured (11424 bits)
> Ethernet II, Src: MS-NLB-PhysServer-26_c5:01:00:00 (02:1a:c5:01:00:00), Dst: MS-NLB          02:1a:c5:04:00:00)
> Internet Protocol Version 4, Src: 10.1.2.1, Dst: 81.192.52.198
> Transmission Control Protocol, Src Port: 3085, Dst Port: 80, Seq: 20825636, Ack: 1,
> [14620 Reassembled TCP Segments (20826997 bytes): #9095(1448), #9096(1448), #9099(1          3), #9104(1448), #9107(1448), #9108(1448), #9111(1448), #9112(1448), #9115
> Hypertext Transfer Protocol
> HTML Form URL Encoded: application/x-www-form-urlencoded
```

Figure 4. Decode packets without download using the built-in, browser-based packet analyzer based. on Wireshark®.

For more information on the Endace portfolio of products, visit: endace.com/products

For further information, email: info@endace.com