LiveAction®

ThreatEye

How-To Guide: Intelligent PCAP

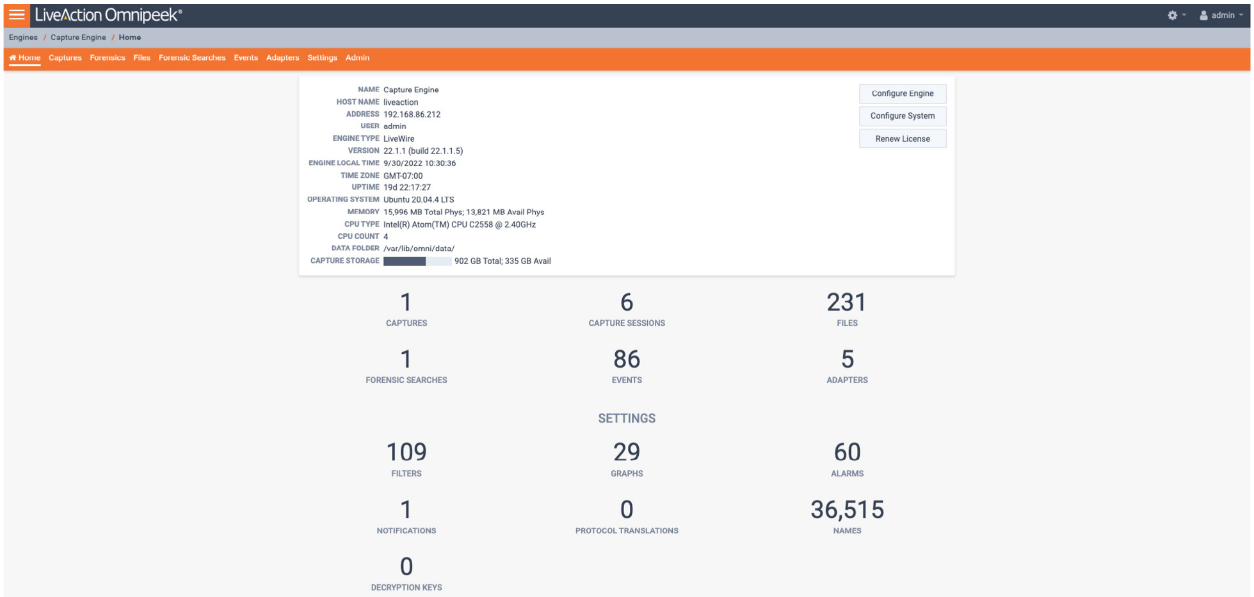
How to Apply Intelligent Packet Capture

How to Apply Intelligent Packet Capture

Intelligent packet capture is easy to configure yet extremely powerful.

The below screenshot is the web view of the Omnipeek UI. It manages all LiveAction appliances, including LiveWire Edge, LiveWire Core, Power Core or LiveWire virtual. As soon as a LiveWire is purchased, go to the to the IP address associated and this UI will pop up on the home page.

This is the “Home” view:


LiveAction Omnipeek®
admin
Engines / Capture Engine / Home
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin
Configure Engine
Configure System
Renew License

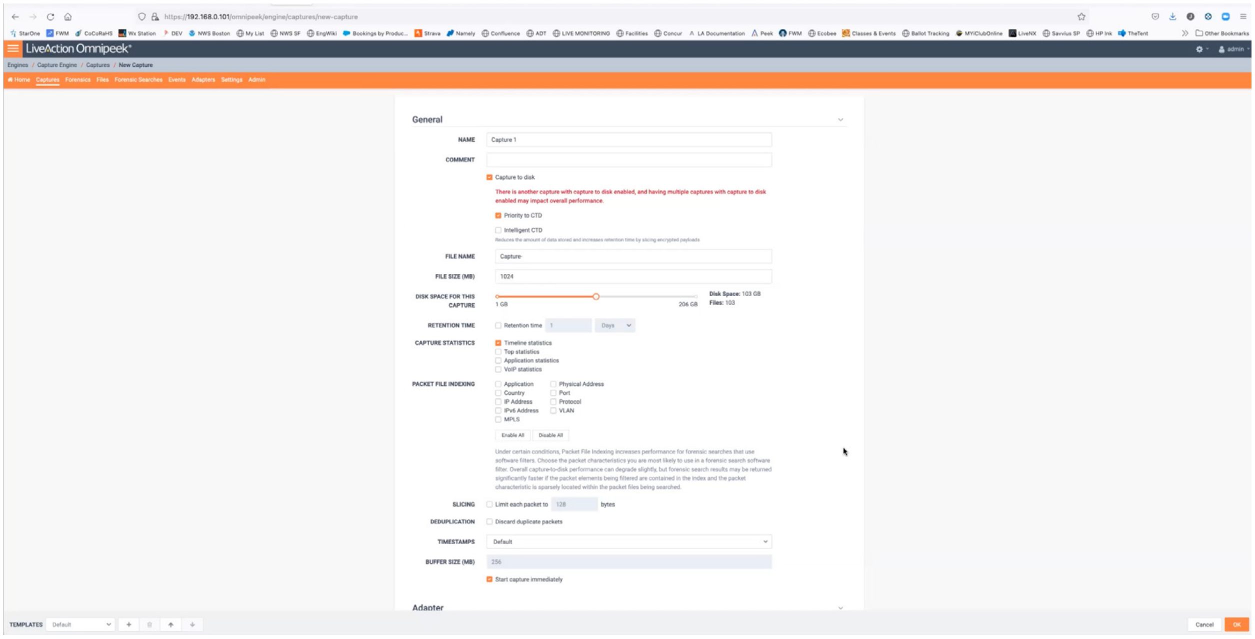
NAME Capture Engine
HOST NAME liveaction
ADDRESS 192.168.86.212
USER admin
ENGINE TYPE LiveWire
VERSION 22.1.1 (build 22.1.1.5)
ENGINE LOCAL TIME 9/30/2022 10:30:36
TIME ZONE GMT-07:00
UPTIME 19d 22:17:27
OPERATING SYSTEM Ubuntu 20.04.4 LTS
MEMORY 15,996 MB Total Phys; 13,821 MB Avail Phys
CPU TYPE Intel(R) Atom(TM) CPU C2558 @ 2.40GHz
CPU COUNT 4
DATA FOLDER /var/lib/omni/data/
CAPTURE STORAGE 902 GB Total; 335 GB Avail

1 CAPTURES
6 CAPTURE SESSIONS
231 FILES
1 FORENSIC SEARCHES
86 EVENTS
5 ADAPTERS

SETTINGS

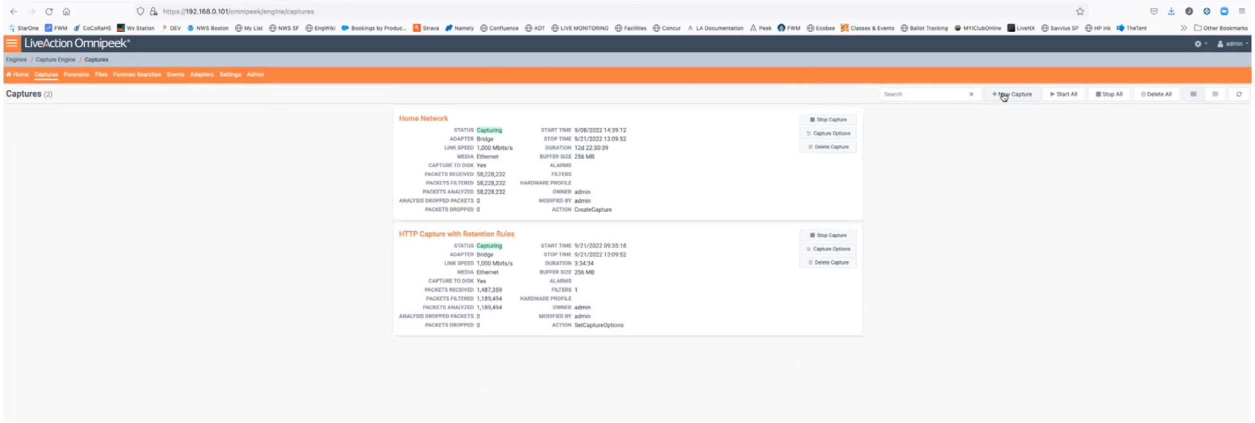
109 FILTERS
29 GRAPHS
60 ALARMS
1 NOTIFICATIONS
0 PROTOCOL TRANSLATIONS
36,515 NAMES
0 DECRYPTION KEYS

Let’s move to the “Captures” view:


https://192.168.0.101/omnipeek/engine/captures/new-capture
LiveAction Omnipeek®
admin
Engines / Capture Engine / Captures / New Capture
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin
General
Adapter
Enable All
Disable All
TEMPLATES
Cancel
OK

NAME Capture 1
COMMENT
☑ Capture to disk
There is another capture with capture to disk enabled, and having multiple captures with capture to disk enabled may impact overall performance.
☑ Priority to CTD
☐ Intelligent CTD
Reduces the amount of data stored and increases retention time by slicing encrypted payloads
FILE NAME Capture-
FILE SIZE (MB) 1024
DISK SPACE FOR THIS CAPTURE 1 GB 206 GB Disk Space: 103 GB Files: 103
RETENTION TIME ☐ Retention time 1 Days
CAPTURE STATISTICS ☑ Timeline statistics ☐ Top statistics ☐ Application statistics ☐ VoIP statistics
PACKET FILE INDEXING ☐ Application ☐ Country ☐ IP Address ☐ IPv6 Address ☐ MPLS ☐ Physical Address ☐ Port ☐ Protocol ☐ VLAN
Under certain conditions, Packet File Indexing increases performance for forensic searches that use software filters. Choose the packet characteristics you are most likely to use in a forensic search software filter. Overall capture-to-disk performance can degrade slightly, but forensic search results may be returned significantly faster if the packet elements being filtered are contained in the index and the packet characteristic is sparsely located within the packet files being searched.
SLICING ☐ Limit each packet to 128 bytes
DEDUPLICATION ☐ Discard duplicate packets
TIMESTAMPS Default
BUFFER SIZE (MB) 256
☑ Start capture immediately
TEMPLATES Default

The "Captures" area shows current captures. On the right-hand side, you can select the box for "+ New Capture"



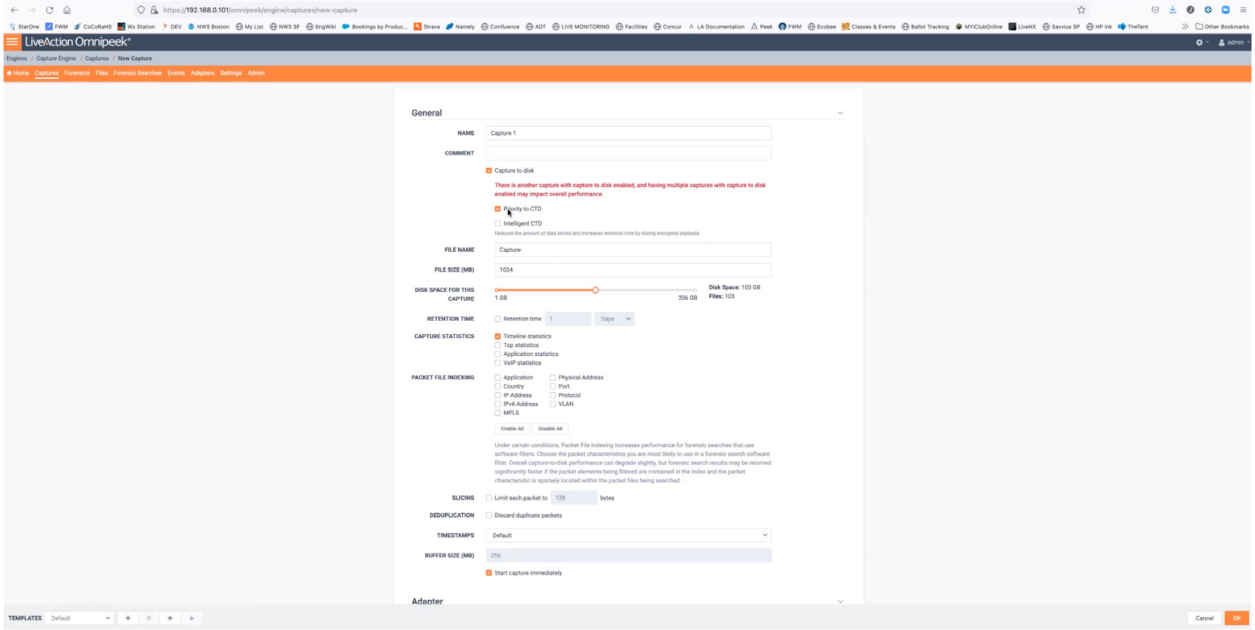
Home Network

STATUS Capturing
ADAPTER Bridge
LINK SPEED 1,000 Mbits/s
MEDIA Ethernet
CAPTURE TO DISK Yes
PACKETS RECEIVED 58,228,232
PACKETS FILTERED 58,228,232
PACKETS ANALYZED 58,228,232
ANALYSIS DROPPED PACKETS 0
PACKETS DROPPED 0
START TIME 9/08/2022 14:39:12
STOP TIME 9/21/2022 13:09:52
DURATION 12d 22:30:39
BUFFER SIZE 256 MB
ALARMS
FILTERS
HARDWARE PROFILE
OWNER admin
MODIFIED BY admin
ACTION CreateCapture

HTTP Capture with Retention Rules

STATUS Capturing
ADAPTER Bridge
LINK SPEED 1,000 Mbits/s
MEDIA Ethernet
CAPTURE TO DISK Yes
PACKETS RECEIVED 1,487,359
PACKETS FILTERED 1,189,494
PACKETS ANALYZED 1,189,494
ANALYSIS DROPPED PACKETS 0
PACKETS DROPPED 0
START TIME 9/21/2022 09:35:18
STOP TIME 9/21/2022 13:09:52
DURATION 3:34:34
BUFFER SIZE 256 MB
ALARMS
FILTERS 1
HARDWARE PROFILE
OWNER admin
MODIFIED BY admin
ACTION SetCaptureOptions

Within the " + New Capture" view, there is an option to select "Intelligent CTD". This stands for Capture to Disc. Check the box to turn it on. Once a new data capturing session begins, the Intelligent Packet Capture setting will be applied.



General

NAME Capture 1

COMMENT

☑ Capture to disk

There is another capture with capture to disk enabled, and having multiple captures with capture to disk enabled may impact overall performance.

☑ Priority to CTD

☐ Intelligent CTD

Reduces the amount of data stored and increases retention time by slicing encrypted payloads

FILE NAME Capture-

FILE SIZE (MB) 1024

DISK SPACE FOR THIS CAPTURE 1 GB 206 GB Disk Space: 103 GB Files: 103

RETENTION TIME ☐ Retention time 1 Days

CAPTURE STATISTICS
☑ Timeline statistics
☐ Top statistics
☐ Application statistics
☐ VoIP statistics

PACKET FILE INDEXING
☐ Application ☐ Physical Address
☐ Country ☐ Port
☐ IP Address ☐ Protocol
☐ IPv6 Address ☐ VLAN
☐ MPLS

Under certain conditions, Packet File Indexing increases performance for forensic searches that use software filters. Choose the packet characteristics you are most likely to use in a forensic search software filter. Overall capture-to-disk performance can degrade slightly, but forensic search results may be returned significantly faster if the packet elements being filtered are contained in the index and the packet characteristic is sparsely located within the packet files being searched.

SLICING ☐ Limit each packet to 128 bytes

DEDUPLICATION ☐ Discard duplicate packets

TIMESTAMPS Default

BUFFER SIZE (MB) 256

☑ Start capture immediately

Adapter

What does Intelligent Packet Capture do?

Intelligent Packet Capture slices off the encrypted portion of the packet at the payload. Most traffic that travels across the web today is encrypted, HTTPS using SSL. In most cases, the customer does not have the appropriate key to decrypt the data, resulting in storage space used for encrypted data that is useless to the customer and that could be reallocated to longer data retention times.

Why is It Called Intelligent Packet Capture?

The reason we call it intelligent is for two reasons:

1. LiveWire is smart enough to recognize which flows have encrypted payloads and which internet protocol is being communicated.
2. LiveWire is smart enough to know where to slice the packet to leave a full packet header. The header is a different size depending on the protocol used. For example, for HTTP the packet is sliced after the 64th bite or if it’s e-mail, it’s sliced after the 32nd bite.