

Packet Capture on the EH1000v/2000v with VMware

This guide describes how to use packet capture on the EH1000v/2000v virtual appliances with VMware. The guide assumes experience administering VMware ESX and ESXi environments. Users must have access to the ExtraHop Admin UI and write permission to the ExtraHop Web UI in order to complete the steps in this guide.






Best practices:

- Use a storage partition on a local machine.
- Use a minimum disk size of 1 GB

Enabling Packet Capture

Ensure that your ExtraHop license has packet capture enabled.

1. In the Admin UI, go to **System Settings** and click **License**.

System Settings	
Services	 Change
Firmware	 Change
System Time	 Change
Shutdown/Restart	 Change
License	 Change

2. Go to the **Features** section and verify that packet capture is enabled. If packet capture is enabled, go to the next section. If your license does not have packet capture enabled, go to the next step.

Features	
Activity Map	Enabled
Device Safety Limit	1000
License Server Required	Enabled
Packet Capture	Enabled
SSL Decryption	Enabled
Triggers	Enabled

3. The ExtraHop requires a product key and a license in order to use packet capture. Contact ExtraHop Support (support@extrahop.com) to obtain your product key.

- a. Go to **Manage License** and click **Register** to enter the product key.
- b. Enter the product key and then click **Register**. The ExtraHop system now contacts the license server and validates the product key. After the product key is validated, the license is downloaded.

Register Appliance

Product Key:

- c. Refresh your browser to see the updated license.

The following example shows a properly licensed ExtraHop with packet capture on the **License Administration** page of the Admin UI:

License Administration	
System Information	
Dossier	94dac934b909ed6fc719c9f5a7b788dc
Serial	vmw564d1051fdebda52ce7f68a631f17ecc
Product Key	EXTR-EXTR-KTSX-C5WB
Platform	EH1000V
Modules	
Name	Status
CIFS	Enabled
DB2	Enabled
DIAMETER	Enabled
FIX	Enabled
HTTP-AMF	Enabled
IBMMQ	Enabled
ICA	Enabled
Interfaces	
10G License	False
Number of Licensed	1
Features	
Activity Map	Enabled
Device Safety Limit	250
License Server Required	Enabled
Packet Capture	Enabled (Dedicated Drive)
Triggers	Enabled

- In the Admin UI, go to **System Settings** and click **Disk**. The Drive Map shows the **No Packet Capture Disk** message.

Direct Connected Disks	
Disk # 0	
Role	Firmware
Status	running
Vendor	VMware
Model	Virtual disk
Media Type	HDD
Size	4.0GB
Disk # 1	
Role	Datastore
Status	running
Vendor	VMware
Model	Virtual disk
Media Type	HDD
Size	250.0GB
Disk # 2	
	No Packet Capture Disk
Role	Packet Capture
Status	Empty
Vendor	Empty
Model	Empty
Media Type	Empty
Size	Empty

5. Log in to VMware and click the **Summary** tab.

ExtraHop

Getting Started | **Summary** | Resource Allocation | Performance | Events | Console | Permissions

General

Guest OS: Other (32-bit)
 VM Version: 7
 CPU: 6 vCPU
 Memory: 6144 MB
 Memory Overhead: 84.50 MB
 VMware Tools: ◆ Not running (Not installed)
 IP Addresses:

DNS Name:
 State: Powered On
 Host: localhost.sea.i.extrahop.com i.extraho...
 Active Tasks:
 vSphere HA Protection: ⊙ N/A ⓘ

Resources

Consumed Host CPU: **36 MHz**
 Consumed Host Memory: **4705.00 MB**
 Active Guest Memory: **184.00 MB** [Refresh Storage Usage](#)
 Provisioned Storage: **260.05 GB**
 Not-shared Storage: **260.05 GB**
 Used Storage: **260.05 GB**

Storage	Drive Type	Capacity
datastore1	Non-SSD	1.08 TB 84%

Network	Type
VM Network 2	Standard port group
VM Network 3	Standard port group
VM Network	Standard port group

Commands

6. Click **Edit Settings**.

Commands

- Power Off
- Suspend
- Reset
- Edit Settings
- Open Console

7. Click **Add**.

ExtraHop - Virtual Machine Properties

Hardware | Options | Resources | Virtual Machine Version: 7

Show All Devices Add... Remove

Hardware	Summary
Memory	6144 MB
CPUs	6
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Network adapter 1	VM Network
Network adapter 2	VM Network 2
Network adapter 3	VM Network 3
Network adapter 4	VM Network 3
USB controller	Present

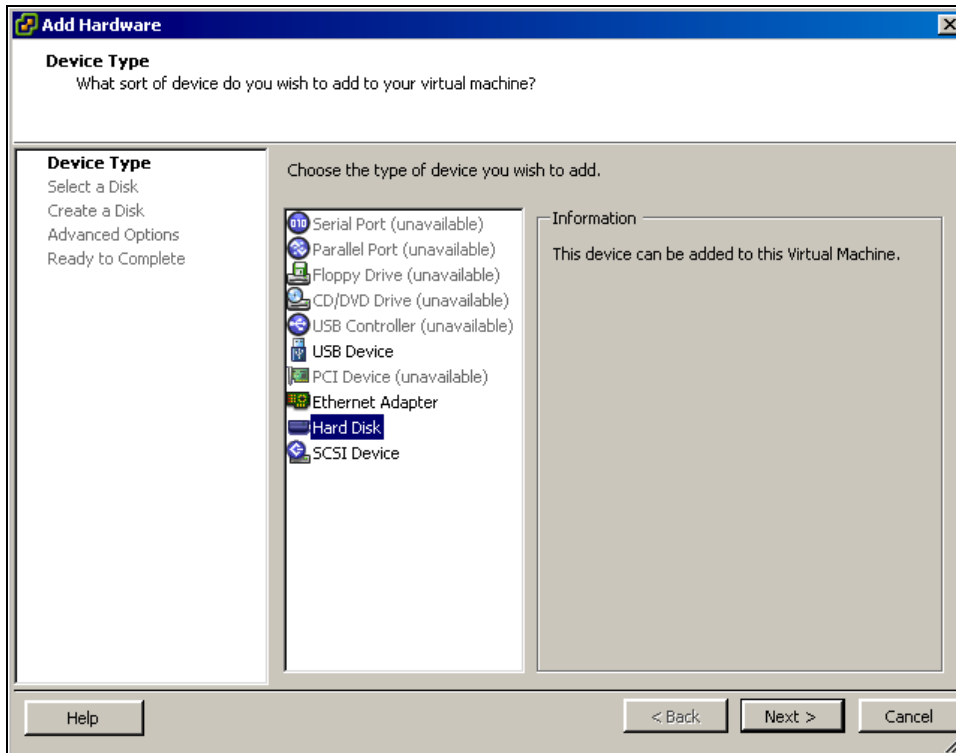
Memory Configuration

Memory Size: GB

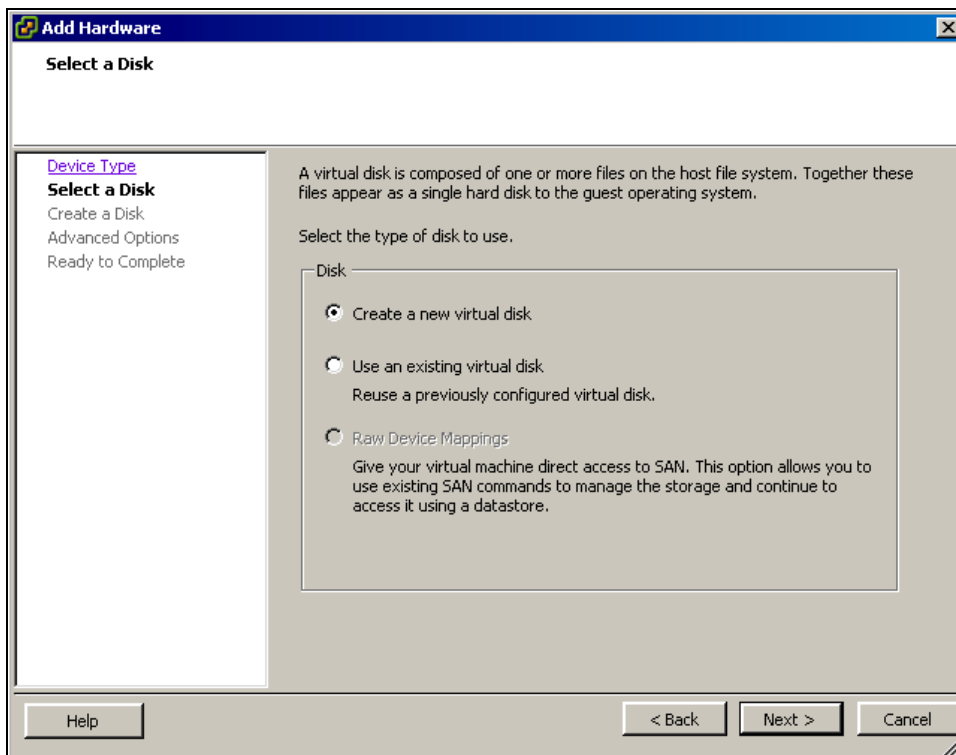
255 GB
128 GB
64 GB
32 GB
16 GB
8 GB
4 GB
2 GB
1 GB

- ▶ Maximum recommended for this guest OS: 64 GB.
- ▶ Maximum recommended for best performance: 24564 MB.
- ▶ Default recommended for this guest OS: 512 MB.
- ▶ Minimum recommended for this guest OS: 32 MB.

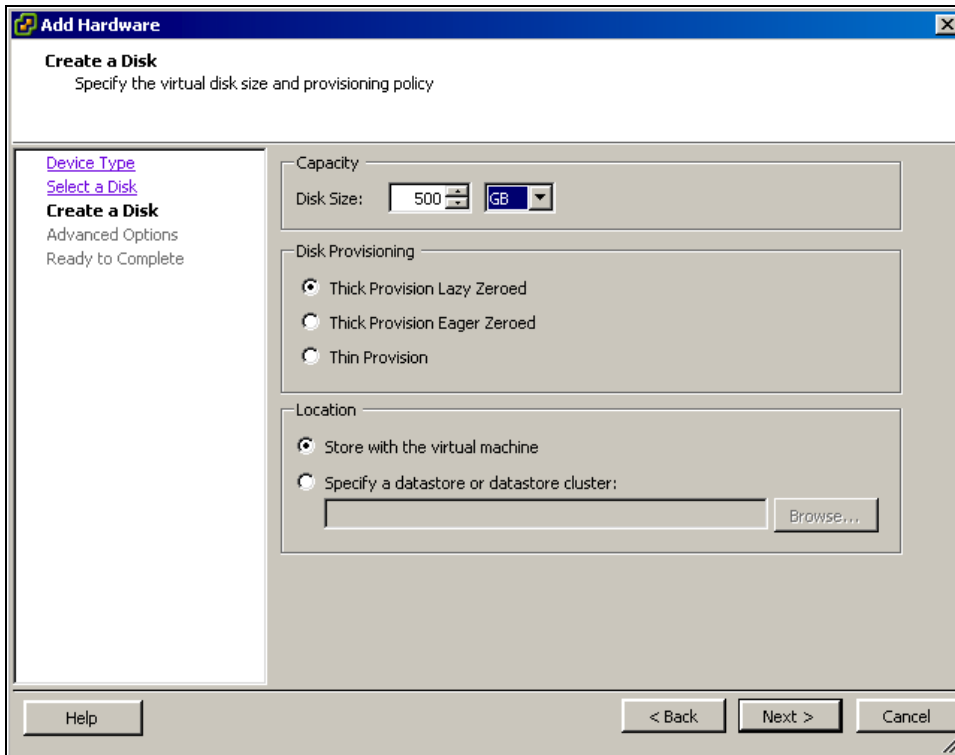
8. Select **Hard Disk** and click **Next**.



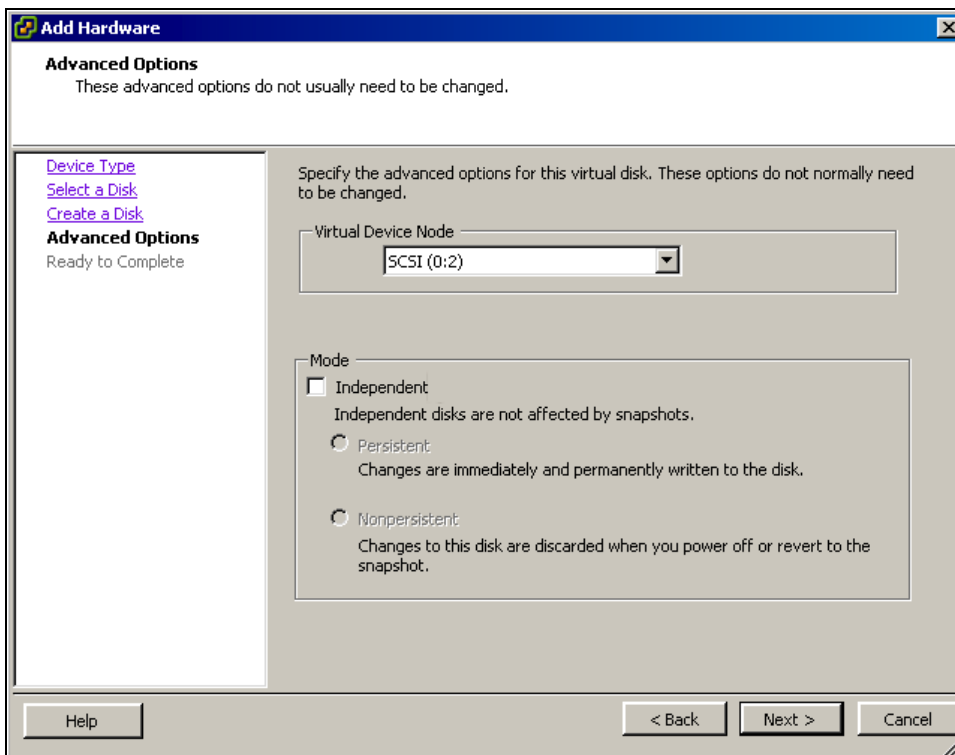
9. Select the **Create a new virtual disk** radio button and click **Next**.



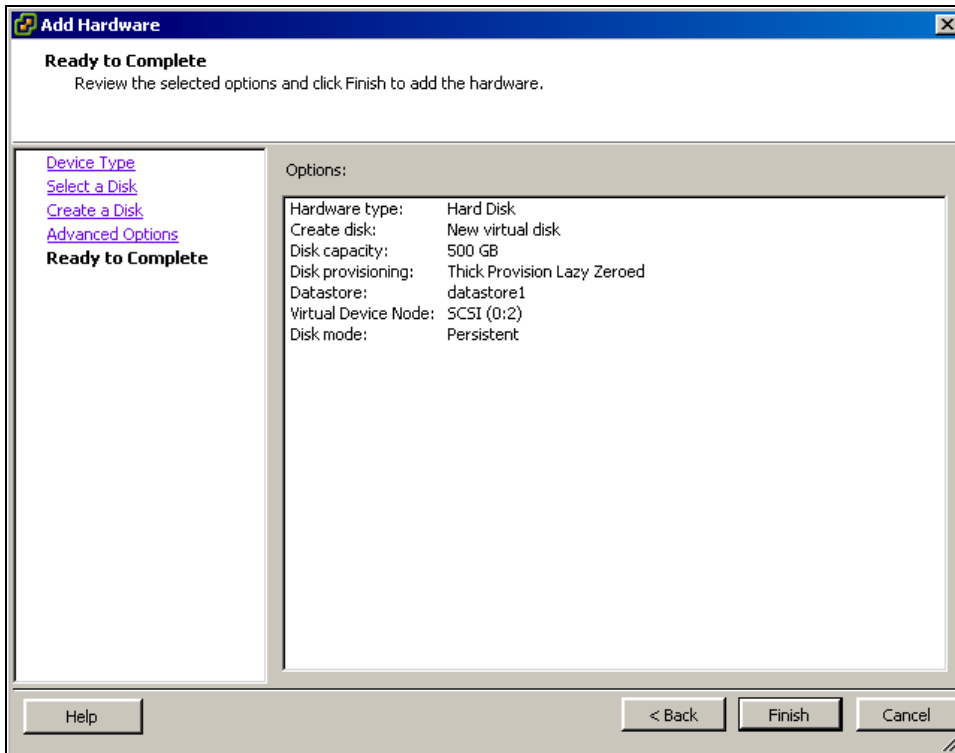
10. Set the **Disk Size** to 500 GB, select the **Thick Provision Lazy Zero** radio button and click **Next**.



11. In the **Advanced Options** window, use the default settings and click **Next**.



12. Click **Finish**.



13. Click **OK**.
14. Refresh the Admin UI. The drive is now allotted for packet capture.
15. Next to **Triggered Packet Capture**, click **Enable**.

Disk # 2	
Role	Packet Capture
Status	running
Vendor	VMware
Model	Virtual disk
Media Type	HDD
Size	500.0GB
Triggered Packet Capture	Enable

16. Wait approximately 10 minutes. When the progress indicator disappears, your VM is ready to use packet capture.

Using Triggers to Define the Packet Capture

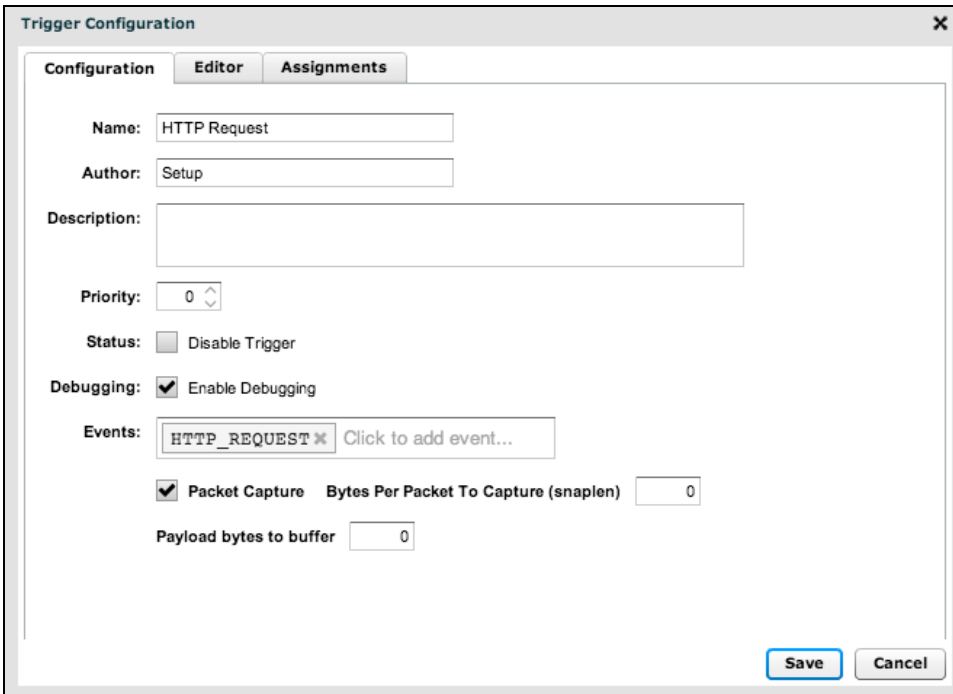
The ExtraHop system uses Application Inspection Triggers to gather custom metrics. These metrics are stored internally and can be used by other features, such as packet capture. Triggers are user-defined scripts that perform additional actions during well-defined events.

For information about writing triggers, refer to the following related documentation :

- *ExtraHop Guide: Getting Started with Application Inspection Triggers.*
- *ExtraHop Application Inspection Triggers API*

To create a trigger, complete the following steps:

1. In the Web UI, click **Settings**, click **Triggers**, and then click **New**.
2. Enter a name for the trigger, select the event that will activate the trigger, and click the **Packet Capture** checkbox.



Once you have tested the trigger to ensure it works, uncheck **Enable Debugging** to avoid excessive debug messages in the Runtime Log.

3. Click the **Editor** tab, enter your trigger source code, and click **Save**.
4. Click the **Assignments** tab and assign the trigger to a device or group of devices.

Viewing the Packet Capture Results

1. In the Admin UI, go to the **Packet Captures** section and click **View & Download Packet Captures**.



2. On the **Packet Captures** page, select a packet capture to download to your workstation. You can filter

packet captures by name and the date of capture.

Packet Captures

Listing options » Name contains: Captured after:

Captured before: Captures per page:

8 packet captures. Showing page 1 of 1

<input type="checkbox"/>	Name	Packets	Bytes	Duration	Start Time	End Time
<input type="checkbox"/>	0.0.0.0.in-addr.arpa-0.0.0.0.in-addr.arpa	15	1260	<1s	2012-11-19 16:54:34	2012-11-19 16:54:34
<input type="checkbox"/>	0.0.0.0.in-addr.arpa-0.0.0.0.in-addr.arpa	15	1260	<1s	2012-11-19 16:54:31	2012-11-19 16:54:31
<input type="checkbox"/>	0.0.0.0.in-addr.arpa-0.0.0.0.in-addr.arpa	15	1260	1s	2012-11-19 16:31:41	2012-11-19 16:31:42
<input type="checkbox"/>	0.0.0.0.in-addr.arpa-0.0.0.0.in-addr.arpa	15	1260	<1s	2012-11-19 16:31:30	2012-11-19 16:31:30
<input type="checkbox"/>	0.0.0.0.in-addr.arpa-0.0.0.0.in-addr.arpa	15	1260	<1s	2012-11-19 16:31:10	2012-11-19 16:31:10
<input type="checkbox"/>	0.0.0.0.in-addr.arpa-0.0.0.0.in-addr.arpa	15	1260	<1s	2012-11-19 16:30:59	2012-11-19 16:30:59
<input type="checkbox"/>	0.0.0.0.in-addr.arpa-0.0.0.0.in-addr.arpa	15	1260	<1s	2012-11-19 16:30:39	2012-11-19 16:30:39
<input type="checkbox"/>	0.0.0.0.in-addr.arpa-0.0.0.0.in-addr.arpa	15	1260	<1s	2012-11-19 16:30:28	2012-11-19 16:30:28

3. Open the downloaded packet capture in a packet analyzer such as Wireshark.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	69.171.229.16	208.79.144.52	TCP	70	http > 54216 [ACK] Seq=1 Ack=1
2	0.062000	69.171.229.16	208.79.144.52	TCP	1518	[TCP segment of a reassembled P
3	0.062000	69.171.229.16	208.79.144.52	TCP	1518	[TCP segment of a reassembled P
4	0.062000	69.171.229.16	208.79.144.52	TCP	1518	[TCP segment of a reassembled P
5	0.063000	69.171.229.16	208.79.144.52	HTTP	1405	HTTP/1.1 200 OK (text/html)
6	0.065000	208.79.144.52	69.171.229.16	TCP	70	54216 > http [ACK] Seq=1 Ack=28
7	0.065000	208.79.144.52	69.171.229.16	TCP	70	54216 > http [ACK] Seq=1 Ack=56
8	75.681000	208.79.144.52	69.171.229.16	HTTP	996	GET /plugins/like.php?api_key=&l
9	75.698000	69.171.229.16	208.79.144.52	TCP	70	http > 54216 [ACK] Seq=5680 Ack=
10	75.746000	69.171.229.16	208.79.144.52	TCP	1518	[TCP segment of a reassembled P
11	75.746000	69.171.229.16	208.79.144.52	TCP	1518	[TCP segment of a reassembled P

▶ Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
 ▶ Ethernet II, Src: Cisco_b1:b5:00 (00:1e:7a:b1:b5:00), Dst: Hewlett_87:36:09 (00:18:71:87:36:09)
 ▶ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 7
 ▶ Internet Protocol Version 4, Src: 69.171.229.16 (69.171.229.16), Dst: 208.79.144.52 (208.79.144.52)
 ▶ Transmission Control Protocol, Src Port: http (80), Dst Port: 54216 (54216), Seq: 1, Ack: 1, Len: 0

```

0000  00 18 71 87 36 09 00 1e 7a b1 b5 00 81 00 00 07  ..q.6... z.....
0010  08 00 45 00 00 34 66 02 40 00 57 06 32 82 45 ab  ..E..4f. @.w.2.E.
0020  e5 10 d0 4f 90 34 00 50 d3 c8 d9 aa c0 b7 31 6e  ...0.4.P .....ln
0030  54 e6 80 10 00 20 0f fe 00 00 01 01 08 0a 68 8a  T.... .. .....h.
0040  a6 b5 1f 93 b7 bc .....
  
```