

# Detecting Lateral Movement Using Sysmon and Splunk

By David French

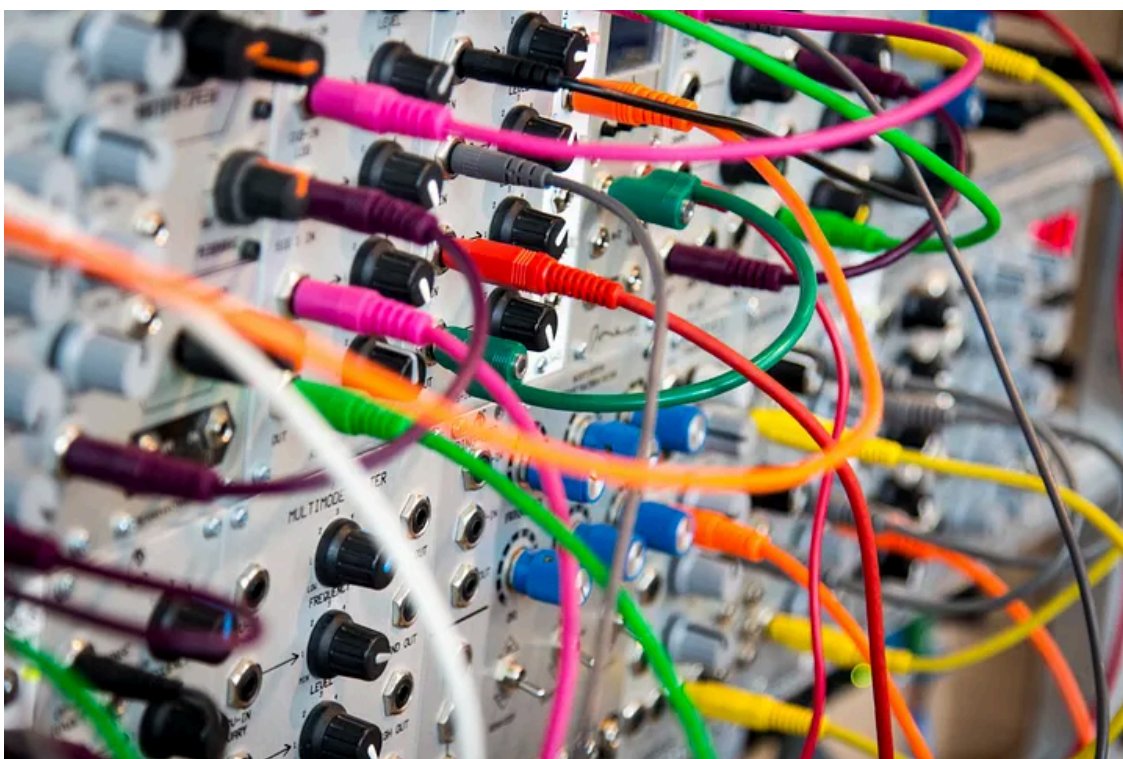
Published: 2020-09-28 · Archived: 2026-04-06 01:57:34 UTC



4 min read

Sep 30, 2018

Press enter or click to view image in full size



Detecting an attacker moving laterally in your environment can be a challenge. It can be difficult to obtain the logs required to identify this activity and differentiate between what is normal versus what is malicious.

This post highlights a few things that you can look for to detect an attacker moving between hosts. With Sysmon installed on Windows hosts and the events being sent to SIEM, you can detect attempts to move laterally and questions during incident response can be answered in minutes versus hours.

Note, if you decide to implement any of the monitoring and detection detailed in this post in a production environment, it's likely that some tuning will be required to filter benign or expected behavior.

## Install and Configure Sysmon on a Windows Host

Download Sysmon and install it on the Windows host as follows.

```
sysmon -i -n
```

Press enter or click to view image in full size

```
C:\Users\buddyholly\Downloads>Sysmon64.exe /?

System Monitor v4.12 - System activity monitor
Copyright (C) 2014-2016 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Usage:
Install:   Sysmon64.exe -i [<configfile>]
           [-h <[sha1!md5!sha256!imphash!*],...>] [-n [<process,...>]]
           [-l [<process,...>]]
Configure: Sysmon64.exe -c [<configfile>]
           [--![-h <[sha1!md5!sha256!imphash!*],...>] [-n [<process,...>]]
           [-l [<process,...>]]]
Uninstall: Sysmon64.exe -u
-c Update configuration of an installed Sysmon driver or dump the
  current configuration if no other argument is provided. Optionally
  take a configuration file.
-h Specify the hash algorithms used for image identification (default
  is SHA1). It supports multiple algorithms at the same time.
  Configuration entry: HashAlgorithms.
-i Install service and driver. Optionally take a configuration file.
-l Log loading of modules. Optionally take a list of processes to track.
-m Install the event manifest (done on service install as well).
-n Log network connections. Optionally take a list of processes to track.
-r Check for signature certificate revocation.
  Configuration entry: CheckRevocation.
-u Uninstall service and driver.

The service logs events immediately and the driver installs as a boot-start
driver to capture activity from early in the boot that the service will write
to the event log when it starts.

On Vista and higher, events are stored in "Applications and Services
Logs/Microsoft/Windows/Sysmon/Operational". On older systems, events are
written to the System event log.

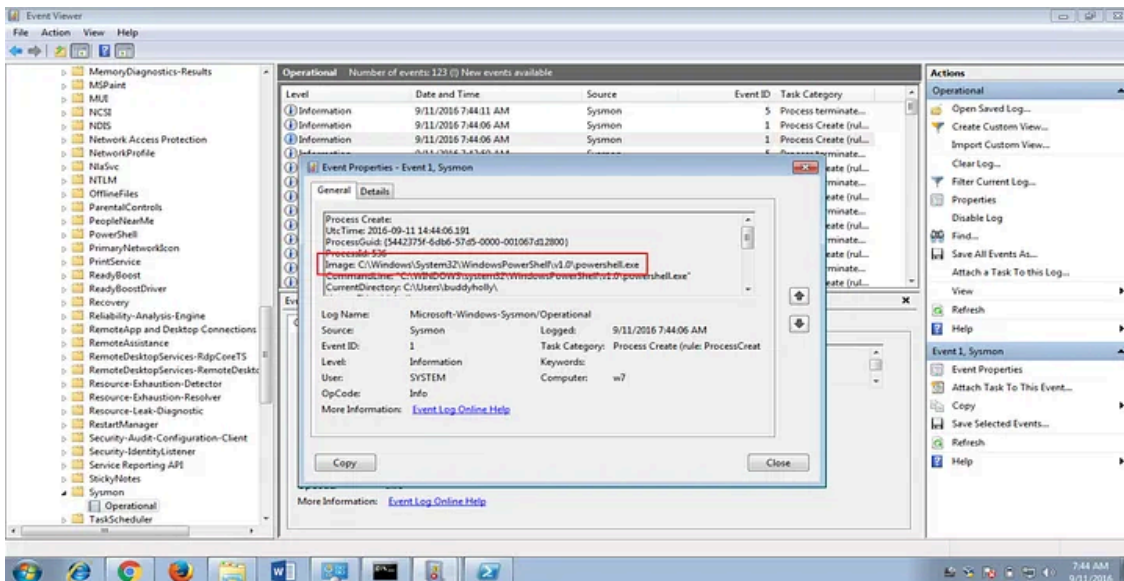
If you need more information on configuration files, use the '-? config'
command. More examples are available on the Sysinternals website.

Specify -accepteula to automatically accept the EULA on installation,
otherwise you will be interactively prompted to accept it.

Neither install nor uninstall requires a reboot.
```

You can view Sysmon events locally by opening Event Viewer and navigating to Microsoft — Windows — Sysmon — Operational. You can see that Sysmon logged the creation of a new process, powershell.exe , in the image below.

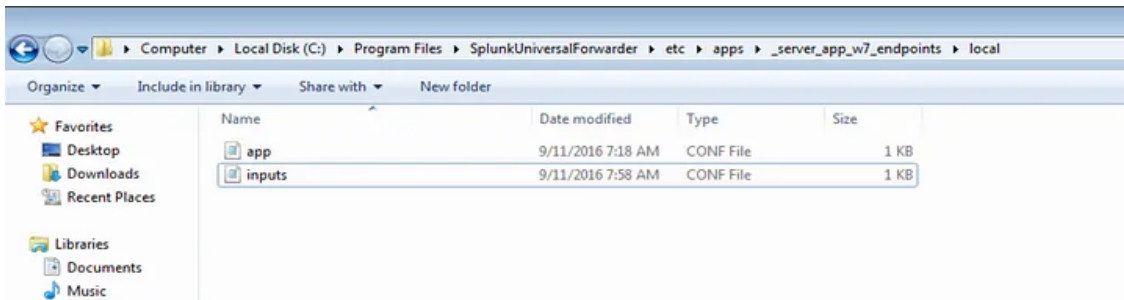
Press enter or click to view image in full size



Add the following text to the inputs.conf file.

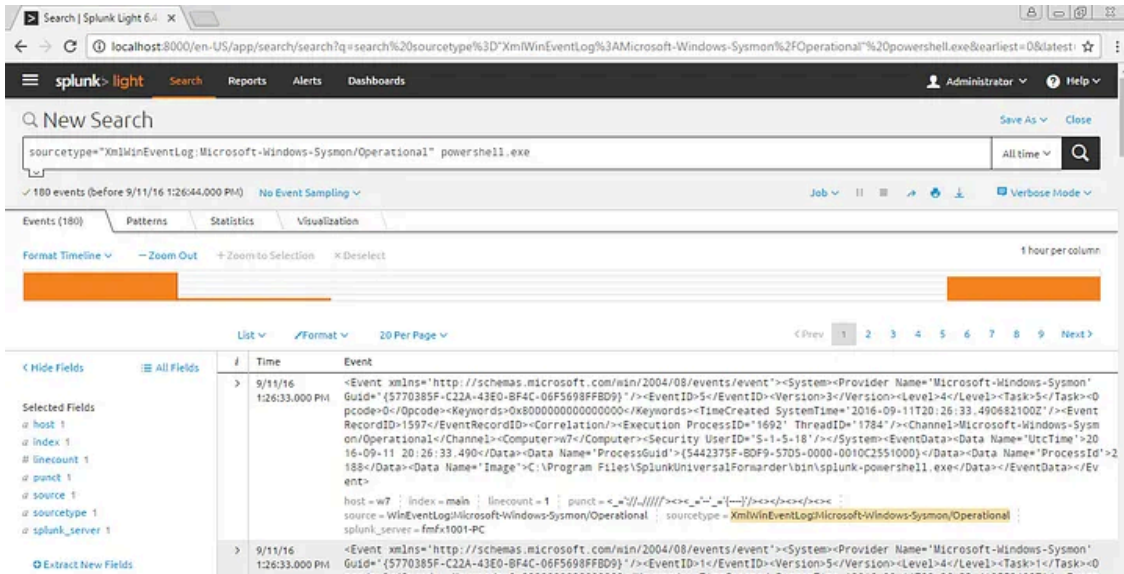
```
[WinEventLog://Microsoft-Windows-Sysmon/Operational]
disabled = false
renderXml = true
```

Press enter or click to view image in full size



Sysmon events from the host can be found in Splunk under `sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"`

Press enter or click to view image in full size

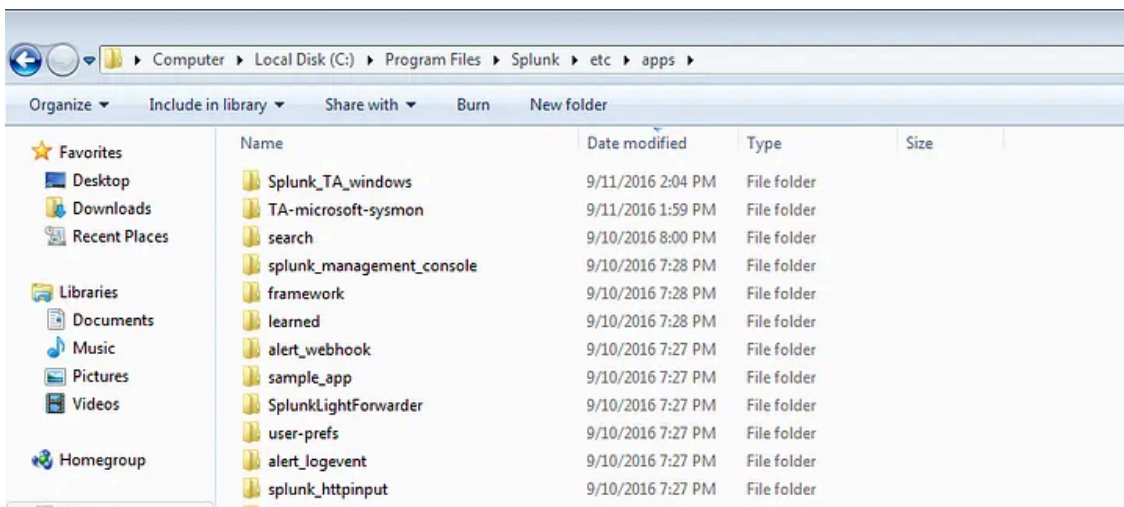


## Install the Splunk “Add-on for Microsoft Sysmon”

Download the add-on from <https://splunkbase.splunk.com/app/1914/#/overview>

Unzip the contents of the compressed file to `C:\Program Files\Splunk\etc\apps` on the Splunk server.

Press enter or click to view image in full size



Restart Splunk Light.

## Get David French’s stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

Events in `sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"` should be parsed into the appropriate fields.



## Detecting an Attacker Establishing SMB Sessions to Move Laterally

The attacker uses the following command or similar to establish a session to the victim.

```
net use \\192.168.1.88
```

Windows Admin Shares is MITRE ATT&CK Technique [T1077](#).

Press enter or click to view image in full size

```
C:\Users\buddyholly>net use \\192.168.1.88
The command completed successfully.

C:\Users\buddyholly>net use
New connections will be remembered.

Status          Local          Remote          Network
-----
OK               \\192.168.1.88\IPC$  Microsoft Windows Network
The command completed successfully.
```

Search sysmon events in Splunk to identify the suspicious SMB (Port 445) session established between the two Windows hosts. See the search string below.

```
sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" 192.168.1.90 445
| table _time, EventCode, EventDescription, host, SourceIp, src_port, User, DestinationIp, DestinationPort, Image, ProcessID, Protocol
```

Press enter or click to view image in full size



Execute `netstat -nao | find "ESTABLISHED"` on the victim computer to view the established SMB session to the attacker.

Press enter or click to view image in full size

```
C:\Users\buddyholly>netstat -nao | find "ESTABLISHED"
TCP        192.168.1.88:445           192.168.1.90:49198      ESTABLISHED    4
TCP        192.168.1.88:49157        192.168.1.81:9997       ESTABLISHED    1536
```

Is it normal for a SMB session to be established between these two hosts? Analyze events in your environment, understand what is normal in terms of process creation/termination and network connections established between hosts, and have your analysts investigate and identify abnormal activity.

## Detecting an Attacker Using PowerShell to Move Laterally

Windows RemoteManagement (WinRM) traffic initiated via PowerShell will be transmitted over ports 5985 and 5986.

Windows Remote Management is MITRE ATT&CK Technique [T1028](#).

In this example, the attacker executes the commands below to remotely execute scripts on the victim or establish a connection to the victim.

Press enter or click to view image in full size

```
PS C:\Users\buddyholly> Invoke-Command -ComputerName w7 -ScriptBlock { ping 8.8.8.8 }
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=48ms TTL=55
Reply from 8.8.8.8: bytes=32 time=44ms TTL=55
Reply from 8.8.8.8: bytes=32 time=44ms TTL=55
Reply from 8.8.8.8: bytes=32 time=42ms TTL=55

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 42ms, Maximum = 48ms, Average = 44ms
PS C:\Users\buddyholly> Invoke-Command -ComputerName w7 -ScriptBlock { systeminfo }
Host Name:                W7
OS Name:                   Microsoft Windows 7 Enterprise
OS Version:                6.1.7601 Service Pack 1 Build 7601
OS Manufacturer:          Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:              Multiprocessor Free
Registered Owner:          buddyholly
Registered Organization:
Product ID:                 55041-051-0236406-86894
Original Install Date:      7/5/2016, 9:15:54 PM
System Boot Time:           9/11/2016, 4:58:27 PM
System Manufacturer:        innotek GmbH
```

In Splunk, we can see the following Sysmon events to identify the suspicious activity.

We can see WinRM traffic from the attacker to the victim over port 5985.

```
sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" 5985 OR 5986
| table _time, EventCode, EventDescription, host, SourceIp, src_port, User, DestinationIp, DestinationPort, Image
```

Press enter or click to view image in full size

The screenshot shows a Splunk search interface with the following search query: `sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" 5985 OR 5986 | table _time, EventCode, EventDescription, host, SourceIp, src_port, User, DestinationIp, DestinationPort, Image`. The results table displays 12 events, all of which are 'Network Connect' events. The columns include \_time, EventCode (3), EventDescription (Network Connect), host (w7), SourceIp (192.168.1.88), src\_port (5985), User (NT AUTHORITY\SYSTEM), DestinationIp (192.168.1.90), DestinationPort (49512, 49511, 49510, 49509, 49508), and Image (System).

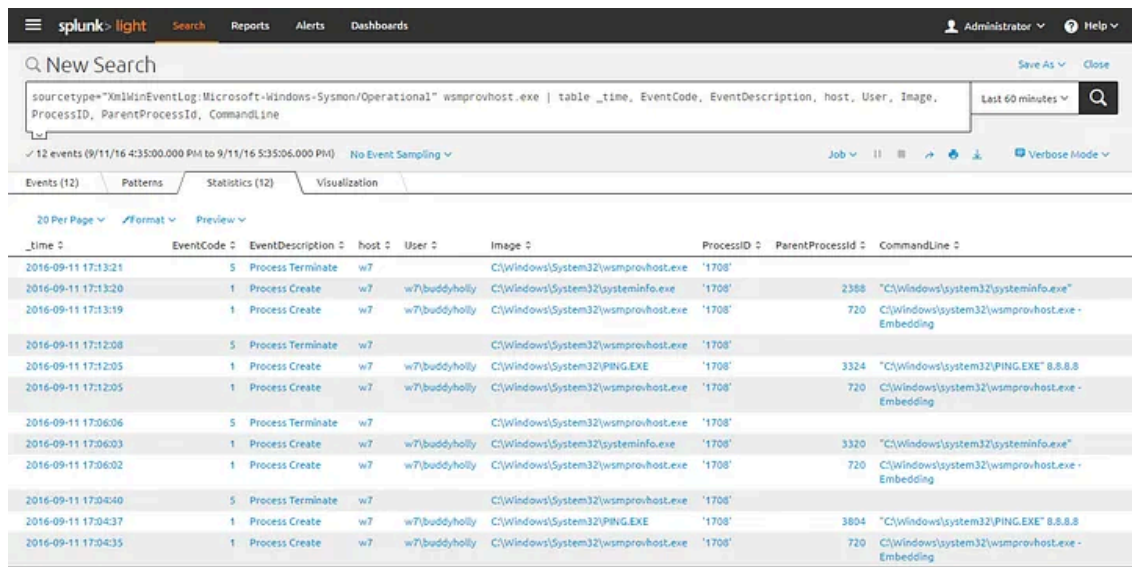
_time	EventCode	EventDescription	host	SourceIp	src_port	User	DestinationIp	DestinationPort	Image
2016-09-11 17:13:21	3	Network Connect	w7	192.168.1.88	5985	NT AUTHORITY\SYSTEM	192.168.1.90	49512	System
2016-09-11 17:13:20	3	Network Connect	w7	192.168.1.88	5985	NT AUTHORITY\SYSTEM	192.168.1.90	49511	System
2016-09-11 17:12:09	3	Network Connect	w7	192.168.1.88	5985	NT AUTHORITY\SYSTEM	192.168.1.90	49510	System
2016-09-11 17:12:06	3	Network Connect	w7	192.168.1.88	5985	NT AUTHORITY\SYSTEM	192.168.1.90	49509	System
2016-09-11 17:12:06	3	Network Connect	w7	192.168.1.88	5985	NT AUTHORITY\SYSTEM	192.168.1.90	49508	System

We can see the WinRM Remote PowerShell process (wsmprovhost.exe) on the victim start the ping.exe and systeminfo.exe processes. We can also see the strings entered on the command line. Would this behavior be

normal in your environment?

```
sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" wsmprovhost.exe  
| table _time, EventCode, EventDescription, host, Image, ProcessID, ParentProcessID, CommandLine
```

Press enter or click to view image in full size



The screenshot shows the Splunk interface with a search query: `sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" wsmprovhost.exe | table _time, EventCode, EventDescription, host, User, Image, ProcessID, ParentProcessID, CommandLine`. The results are displayed in a table with 12 events. The table columns are: `_time`, `EventCode`, `EventDescription`, `host`, `User`, `Image`, `ProcessID`, `ParentProcessID`, and `CommandLine`. The events show a sequence of process terminations and creations for `wsmprovhost.exe` and `systeminfo.exe` on host `w7` by user `w7\buddyholly`. The `CommandLine` for the `systeminfo.exe` processes includes `"C:\Windows\system32\PING.EXE" 8.8.8.8`.

_time	EventCode	EventDescription	host	User	Image	ProcessID	ParentProcessID	CommandLine
2016-09-11 17:13:21	5	Process Terminate	w7		C:\Windows\System32\wsmprovhost.exe	'1708'		
2016-09-11 17:13:20	1	Process Create	w7	w7\buddyholly	C:\Windows\System32\systeminfo.exe	'1708'	2388	"C:\Windows\system32\systeminfo.exe"
2016-09-11 17:13:19	1	Process Create	w7	w7\buddyholly	C:\Windows\System32\wsmprovhost.exe	'1708'	720	C:\Windows\system32\wsmprovhost.exe - Embedding
2016-09-11 17:12:08	5	Process Terminate	w7		C:\Windows\System32\wsmprovhost.exe	'1708'		
2016-09-11 17:12:05	1	Process Create	w7	w7\buddyholly	C:\Windows\System32\PING.EXE	'1708'	3324	"C:\Windows\system32\PING.EXE" 8.8.8.8
2016-09-11 17:12:05	1	Process Create	w7	w7\buddyholly	C:\Windows\System32\wsmprovhost.exe	'1708'	720	C:\Windows\system32\wsmprovhost.exe - Embedding
2016-09-11 17:06:06	5	Process Terminate	w7		C:\Windows\System32\wsmprovhost.exe	'1708'		
2016-09-11 17:06:03	1	Process Create	w7	w7\buddyholly	C:\Windows\System32\systeminfo.exe	'1708'	3320	"C:\Windows\system32\systeminfo.exe"
2016-09-11 17:06:02	1	Process Create	w7	w7\buddyholly	C:\Windows\System32\wsmprovhost.exe	'1708'	720	C:\Windows\system32\wsmprovhost.exe - Embedding
2016-09-11 17:04:40	5	Process Terminate	w7		C:\Windows\System32\wsmprovhost.exe	'1708'		
2016-09-11 17:04:37	1	Process Create	w7	w7\buddyholly	C:\Windows\System32\PING.EXE	'1708'	3804	"C:\Windows\system32\PING.EXE" 8.8.8.8
2016-09-11 17:04:35	1	Process Create	w7	w7\buddyholly	C:\Windows\System32\wsmprovhost.exe	'1708'	720	C:\Windows\system32\wsmprovhost.exe - Embedding

It is possible that the above activity happens often in your environment, which can make it challenging to differentiate between expected and malicious activity. Attackers will use tools that are native to the OS in the hope that their activities go unnoticed. It is important to be familiar with what's normal in your environment and monitor for behavior that is out of the ordinary.

Source: <https://medium.com/threatpunter/detecting-lateral-movement-using-sysmon-and-splunk-318d3be141bc>