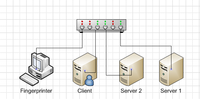
TCP/IP stack fingerprinting

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting#mw-head)[Jump to search](https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting#searchInput)

[](https://en.wikipedia.org/wiki/File:Passive_figure.png)

Passive OS Fingerprinting method and diagram.

**TCP/IP stack fingerprinting** is the passive collection of configuration attributes from a remote device during standard [layer 4](https://en.wikipedia.org/wiki/OSI_model) network communications. The combination of parameters may then be used to infer the remote machine's operating system (aka, **OS fingerprinting**), or incorporated into a [device fingerprint](https://en.wikipedia.org/wiki/Device_fingerprint).



**Contents**

* [1TCP/IP Fingerprint Specifics](https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting#TCP/IP_Fingerprint_Specifics)
* [2Protection against and detecting fingerprinting](https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting#Protection_against_and_detecting_fingerprinting)
* [3Fingerprinting tools](https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting#Fingerprinting_tools)
* [4References](https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting#References)
* [5External links](https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting#External_links)

TCP/IP Fingerprint Specifics[[edit](https://en.wikipedia.org/w/index.php?title=TCP/IP_stack_fingerprinting&action=edit&section=1)]

Certain parameters within the [TCP protocol](https://en.wikipedia.org/wiki/TCP_protocol) definition are left up to the implementation. Different operating systems, and different versions of the same operating system, set different defaults for these values. By collecting and examining these values, one may differentiate among various operating systems, and implementations of TCP/IP. The TCP/IP fields that may vary include the following:

* Initial [packet](https://en.wikipedia.org/wiki/Network_packet) size (16 bits)
* Initial [TTL](https://en.wikipedia.org/wiki/Time_to_live) (8 bits)
* Window size (16 bits)
* [Max segment size](https://en.wikipedia.org/wiki/Maximum_segment_size) (16 bits)
* Window scaling value (8 bits)
* "don't fragment" flag (1 bit)
* "sackOK" flag (1 bit)
* "nop" flag (1 bit)

These values may be combined to form a 67-bit signature, or fingerprint, for the target machine.[[1]](https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting#cite_note-1) Just inspecting the Initial TTL and window size fields is often enough in order to successfully identify an operating system, which eases the task of performing manual OS fingerprinting.[[2]](https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting#cite_note-2)

Protection against and detecting fingerprinting[[edit](https://en.wikipedia.org/w/index.php?title=TCP/IP_stack_fingerprinting&action=edit&section=2)]

Protection against the fingerprint doorway to attack is achieved by limiting the type and amount of traffic a defensive system responds to. Examples include blocking *address masks* and *timestamps* from outgoing [ICMP](https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol) control-message traffic, and blocking [ICMP echo replies](https://en.wikipedia.org/wiki/ICMP_Echo_Reply). A security tool can alert to potential fingerprinting: it can match another machine as having a fingerprinter configuration by detecting *its* fingerprint.[[3]](https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting#cite_note-3)

Disallowing TCP/IP fingerprinting provides protection from [vulnerability scanners](https://en.wikipedia.org/wiki/Vulnerability_scanner) looking to target machines running a certain operating system. Fingerprinting facilitates attacks. Blocking those ICMP messages is only one of an array of defenses required for full protection against attacks.[[4]](https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting#cite_note-4)

Targeting the ICMP datagram, an obfuscator running on top of IP in the internet layer acts as a "scrubbing tool" to confuse the TCP/IP fingerprinting data. These exist for [MS Windows](https://en.wikipedia.org/wiki/MS_Windows),[[5]](https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting#cite_note-5) [Linux](https://en.wikipedia.org/wiki/Linux)[[6]](https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting#cite_note-6) and [FreeBSD](https://en.wikipedia.org/wiki/FreeBSD).[[7]](https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting#cite_note-7)

Fingerprinting tools[[edit](https://en.wikipedia.org/w/index.php?title=TCP/IP_stack_fingerprinting&action=edit&section=3)]

A list of TCP/OS Fingerprinting Tools

* [Ettercap](https://en.wikipedia.org/wiki/Ettercap_(computing)) – passive TCP/IP stack fingerprinting.
* [NetworkMiner](https://en.wikipedia.org/w/index.php?title=NetworkMiner&action=edit&redlink=1) – passive [DHCP](https://en.wikipedia.org/wiki/DHCP) and TCP/IP stack fingerprinting (combines p0f, Ettercap and Satori databases)
* [Nmap](https://en.wikipedia.org/wiki/Nmap) – comprehensive active stack fingerprinting.
* [p0f](https://en.wikipedia.org/wiki/P0f) – comprehensive passive TCP/IP stack fingerprinting.
* NetSleuth – free passive fingerprinting and analysis tool
* [PacketFence](https://en.wikipedia.org/wiki/PacketFence)[[8]](https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting#cite_note-8) – open source [NAC](https://en.wikipedia.org/wiki/Network_Access_Control) with passive DHCP fingerprinting.
* [PRADS](https://en.wikipedia.org/w/index.php?title=PRADS&action=edit&redlink=1) – Passive comprehensive TCP/IP stack fingerprinting and service detection
* Satori – passive [CDP](https://en.wikipedia.org/wiki/Cisco_Discovery_Protocol), DHCP, ICMP, [HPSP](https://en.wikipedia.org/w/index.php?title=HP_Switch_Protocol&action=edit&redlink=1), [HTTP](https://en.wikipedia.org/wiki/HTTP), TCP/IP and other stack fingerprinting.
* SinFP – single-port active/passive fingerprinting.
* XProbe2 – active TCP/IP stack fingerprinting.
* Device Fingerprint Website[[9]](https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting#cite_note-9) - Displays the passive TCP SYN fingerprint of your browser's computer (or intermediate proxy)
* queso - well-known tool from the late 1990s which is no longer being updated for modern operating systems
* Masscan - Fast scanner that transmits 10 million packets per second

References[[edit](https://en.wikipedia.org/w/index.php?title=TCP/IP_stack_fingerprinting&action=edit&section=4)]

* 1. [**^**](https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting#cite_ref-1) Chuvakin A. and Peikari, C: "Security Warrior.", page 229. O'Reilly Media Inc., 2004.
  2. [**^**](https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting#cite_ref-2) [*"Passive OS Fingerprinting, NETRESEC Network Security Blog"*](http://www.netresec.com/?page=Blog&month=2011-11&post=Passive-OS-Fingerprinting)*. Netresec.com. 2011-11-05. Retrieved 2011-11-25.*
  3. [**^**](https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting#cite_ref-3) [*"iplog"*](http://ojnk.sourceforge.net/stuff/iplog.readme)*. Retrieved 2011-11-25.*
  4. [**^**](https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting#cite_ref-4) [*"OS detection not key to penetration"*](http://seclists.org/pen-test/2007/Sep/0030.html)*. Seclists.org. Retrieved 2011-11-25.*
  5. [**^**](https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting#cite_ref-5) [*"OSfuscate"*](http://www.irongeek.com/i.php?page=security/osfuscate-change-your-windows-os-tcp-ip-fingerprint-to-confuse-p0f-networkminer-ettercap-nmap-and-other-os-detection-tools)*. Irongeek.com. 2008-09-30. Retrieved 2011-11-25.*
  6. [**^**](https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting#cite_ref-6) *Carl-Daniel Hailfinger, carldani@4100XCDT.*[*"IPPersonality"*](http://ippersonality.sourceforge.net/)*. Ippersonality.sourceforge.net. Retrieved 2011-11-25.*
  7. [**^**](https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting#cite_ref-7) [*"Defeating TCP/IP stack fingerprinting"*](http://www.usenix.org/events/sec00/full_papers/smart/smart_html/index.html)*. Usenix.org. 2002-01-29. Retrieved 2011-11-25.*
  8. [**^**](https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting#cite_ref-8) [*"PacketFence"*](http://www.packetfence.org/)*. PacketFence. 2011-11-21. Retrieved 2011-11-25.*
  9. [**^**](https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting#cite_ref-9) [http://noc.to](http://noc.to/) [Archived](https://web.archive.org/web/20130811125909/http:/noc.to/) 2013-08-11 at the [Wayback Machine](https://en.wikipedia.org/wiki/Wayback_Machine)

External links[[edit](https://en.wikipedia.org/w/index.php?title=TCP/IP_stack_fingerprinting&action=edit&section=5)]

* [Remote OS detection via TCP/IP Stack FingerPrinting (2nd Generation)](http://insecure.org/nmap/osdetect/)