**Carnivore**

Carnivore is a name given to a system implemented by the [Federal Bureau of Investigation](http://en.wikipedia.org/wiki/Federal_Bureau_of_Investigation) that is analogous to [wiretapping](http://en.wikipedia.org/wiki/Wiretap) except in this case, [e-mail](http://en.wikipedia.org/wiki/E-mail) and other [communications](http://en.wikipedia.org/wiki/Communication) are being tapped instead of [telephone](http://en.wikipedia.org/wiki/Telephone) conversations. Carnivore was essentially a customizable [packet sniffer](http://en.wikipedia.org/wiki/Packet_sniffer) that could monitor all of a target user's [Internet](http://en.wikipedia.org/wiki/Internet) traffic. It is a form of [policeware](http://en.wikipedia.org/wiki/Policeware). [U.S.](http://en.wikipedia.org/wiki/United_States) government officials will confirm or deny little about the physical or logical workings of Carnivore, but there are some basic facts that are generally agreed upon.

In order to be affected, a [computer](http://en.wikipedia.org/wiki/Computer) must be temporarily connected to a computer physically installed at an [Internet service provider](http://en.wikipedia.org/wiki/Internet_service_provider) (ISP) or other location where it can "sniff" traffic on a [LAN](http://en.wikipedia.org/wiki/Local_area_network) segment to look for email messages in transit. The technology itself is not highly advanced — using a standard packet sniffer and some fairly straightforward filtering (such as a [Perl](http://en.wikipedia.org/wiki/Perl_programming_language) script), one could easily duplicate this functionality. Getting the cooperation of the ISPs or the owner of the LAN onto which Carnivore is to be placed can either be voluntary, illegal, or by court order; however, once a system is in place it is allegedly not allowed to simply capture *every* email that passes through the system — by existing U.S. law, publicly acknowledged USG personnel are required to get a [warrant](http://en.wikipedia.org/wiki/Warrant_%28legal%29) or court order naming specific people or email addresses that may be monitored. When an email passes through that matches the filtering criteria mandated by the warrant, the message is logged along with information on the date, time, origin and destination. This logging is most likely relayed in real time to the FBI but the details are not currently known. All other traffic would presumably be dropped without logging or capture.

There is much speculation and concern regarding the implementation, usage, and possible abuses of Carnivore. [Free speech](http://en.wikipedia.org/wiki/Free_speech) advocates and others interested in [civil rights](http://en.wikipedia.org/wiki/Civil_rights) are concerned over the potential for misuse and infringements on individual's [right to privacy](http://en.wikipedia.org/wiki/Right_to_privacy).

Assistant FBI Director [Donald Kerr](http://en.wikipedia.org/w/index.php?title=Donald_Kerr&action=edit) has been quoted as saying:

The Carnivore device works much like commercial "sniffers" and other network diagnostic tools used by ISPs every day, except that it provides the FBI with a unique ability to distinguish between communications which may be lawfully intercepted and those which may not. For example, if a court order provides for the lawful interception of one type of communication (e.g., e-mail), but excludes all other communications (e.g., online shopping) the Carnivore tool can be configured to intercept only those e-mails being transmitted either to or from the named subject.

It is a very specialized network analyzer or "sniffer" which runs as an application program on a normal personal computer under the Microsoft Windows operating system. It works by "sniffing" the proper portions of network packets and copying and storing only those packets which match a finely defined filter set programmed in conformity with the court order. This filter set can be extremely complex, and this provides the FBI with an ability to collect transmissions which comply with pen register court orders, trap & trace court orders, Title III interception orders, etc.

It is important to distinguish now what is meant by "sniffing." The problem of discriminating between users' messages on the Internet is a complex one. However, this is exactly what Carnivore does. It does NOT search through the contents of every message and collect those that contain certain key words like "bomb" or "drugs." It selects messages based on criteria expressly set out in the court order, for example, messages transmitted to or from a particular account or to or from a particular user.[cryptome.org](http://cryptome.org/carnivore-rf.htm)

The [software](http://en.wikipedia.org/wiki/Computer_software) grew from an earlier FBI project called Omnivore. Omnivore began in February [1997](http://en.wikipedia.org/wiki/1997), and was then rebranded. After prolonged negative coverage in the press, the FBI changed the name of its system from "Carnivore" to the more benign-sounding "DCS1000." DCS is reported to stand for "Digital Collection System"; the system has the same functions as before. The three separate packages Carnivore, Packeteer and CoolMiner, are referred to as the [DragonWare Suite](http://en.wikipedia.org/w/index.php?title=DragonWare_Suite&action=edit).