Comparision of Snort, Suricata and Bro

Comparision item	Snort	Suricata	Bro
Type	NIDS	NIDS	NIDS
Available Since	1998	2009	2003
Signature-based or anomaly-based	Signature-based	Signature-based	Both
License	GPLv2+	GPL	BSD
Written in	C / C++	C	C++
Operating System Support			
Windows	YES	YES	NO
Linux	YES	YES	YES
MAC OS X	NO	YES	YES
FreeBSD	YES	YES	YES
Distributed or standalone	Both	Standalone	Standalone
Multi threading support?	NO	YES	YES
Extendable by custom scripts?	NO	NO	YES
Rule customizing?	YES	YES	YES
Snort VRT Rules Support?	YES	YES	NO
Emerging Threads Rule Support?	YES	YES	NO
Logging Format			
Unified2?	YES	YES	YES
Database?	YES	YES	YES
Database engine	MySQL	MySQL	SQLite
Flat file?	YES	YES	YES
Offline analysis? (pcap)	YES	YES	YES
IPv6 Support?	YES	YES	YES