# SNORT

## OpenSource Intrusion Detection System

## www.snort.org

By Khurram Bhatti
CHASE -06

- Introduction to Snort
- Design
- Architecture
- Snort Configuration
- Building Rules
- Uses of Snort

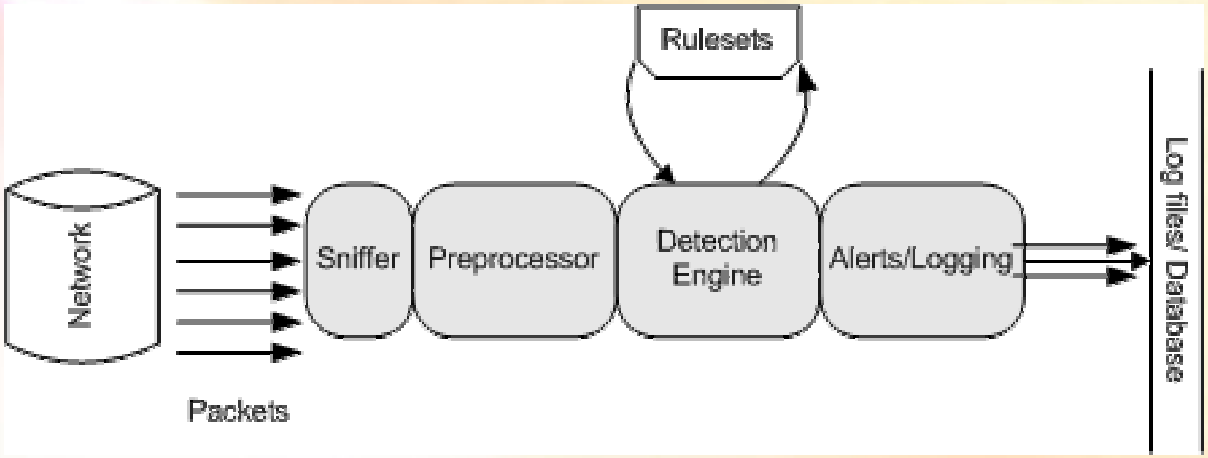
# SNORT -- Introduction

- Snort runs on **multiple** platforms.
- Snort is **configurable**.
- Snort is **free**. Snort is released under the GNU GPL **Open Source network security tool.**
- Snort is **constantly** updated.

## SNORT -- Design

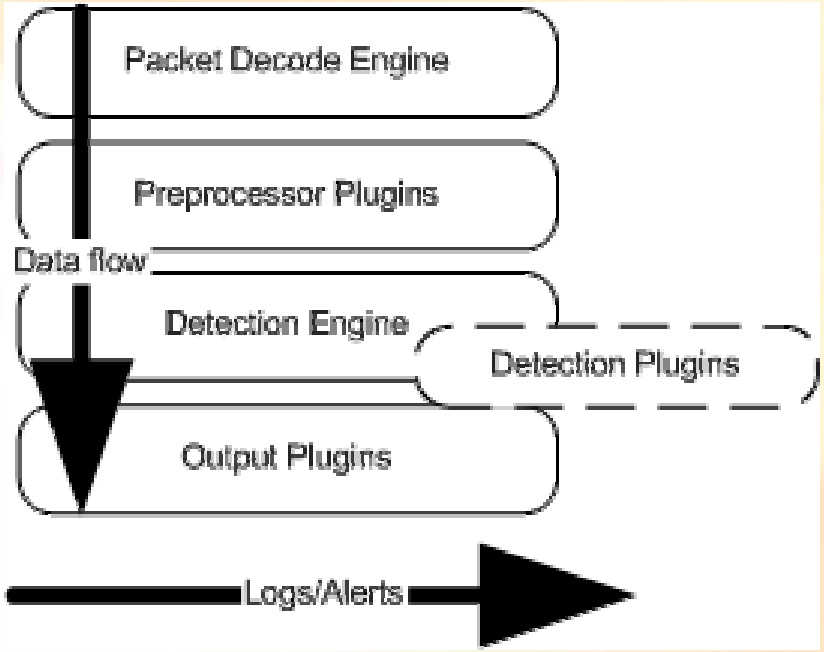
- Packet sniffing network intrusion detection system
- Libpcap-based sniffing interface
- Rules-based detection engine
- Multiple output options
  - decoded logs, tcpdump formatted logs
  - real-time alerting to syslog, file, winpopup

# SNORT -- Architecture



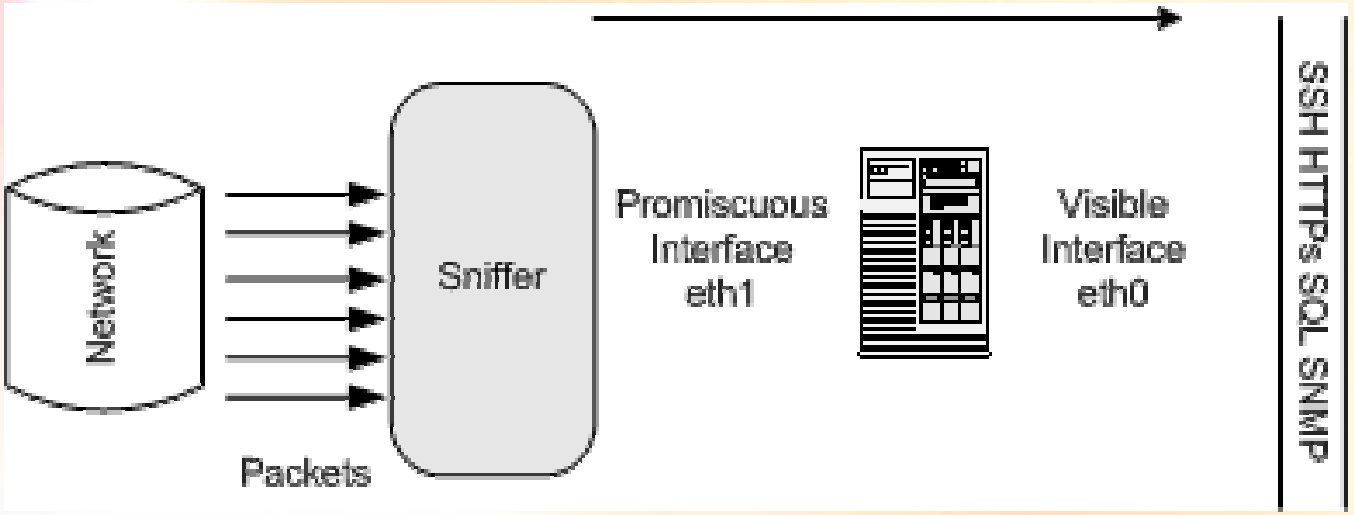

***Architecture of snort***

# SNORT -- Components



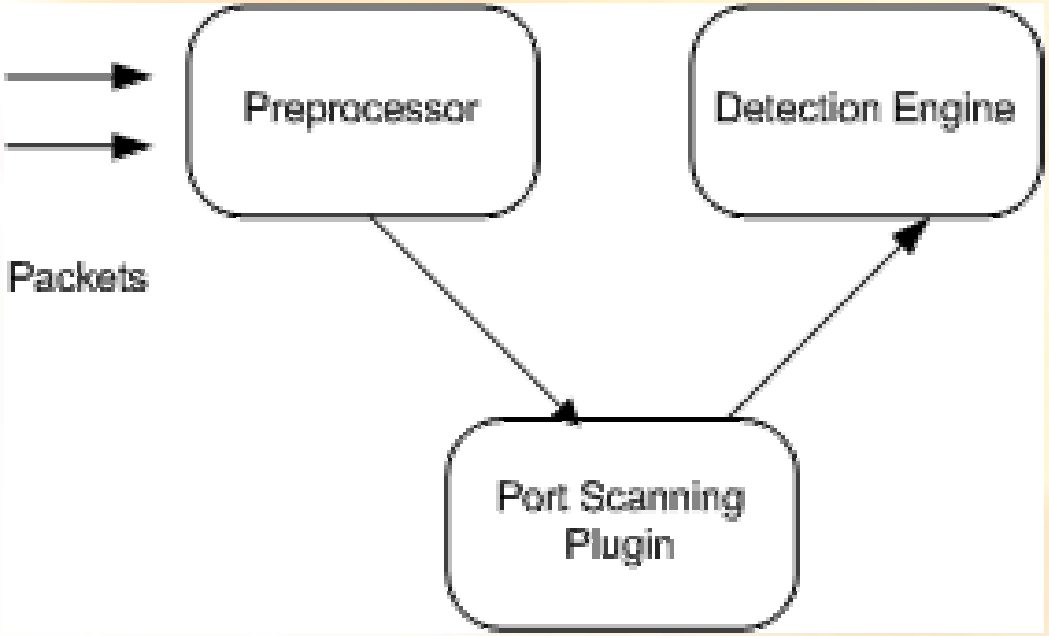

***Data Flow between components***

# SNORT – Sniffer packet flow



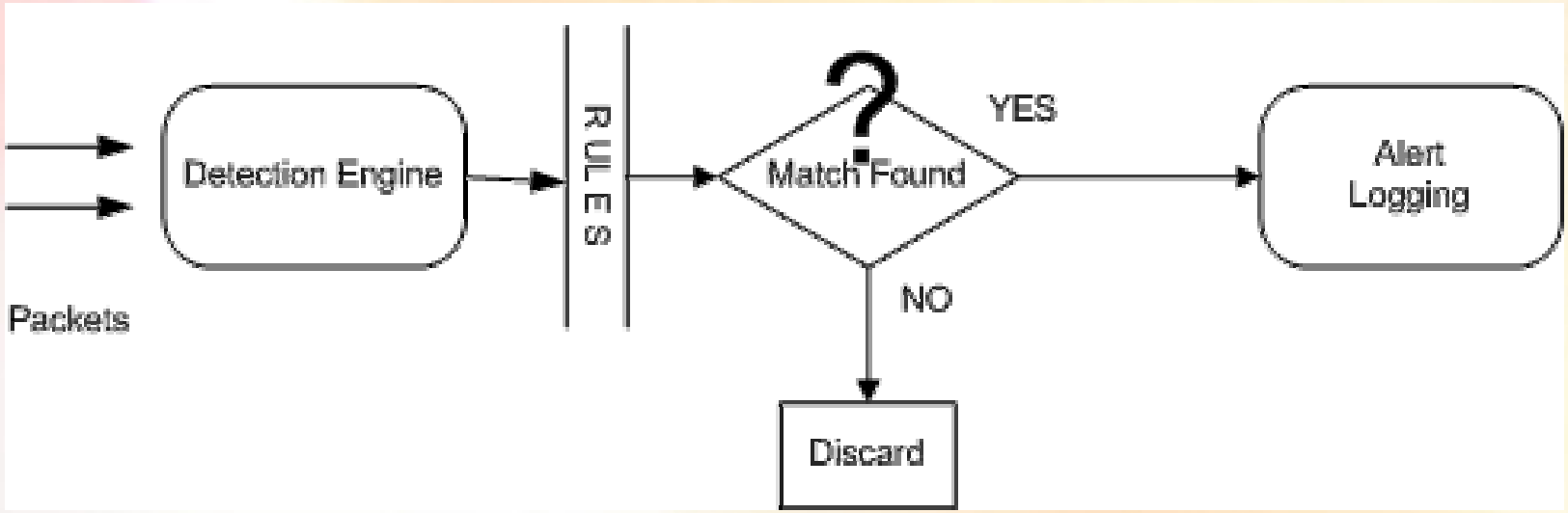

***Sniffer packet flow***

# SNORT – Preprocessor Plugin



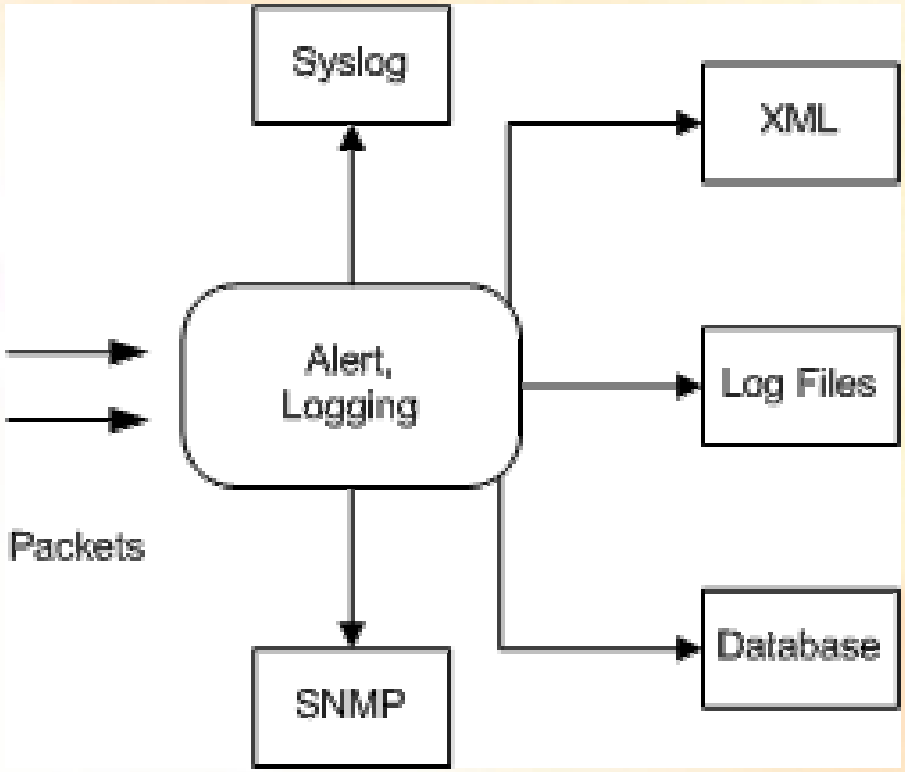

***Packet flow in preprocessor plug-in***

# SNORT – Detection Engine



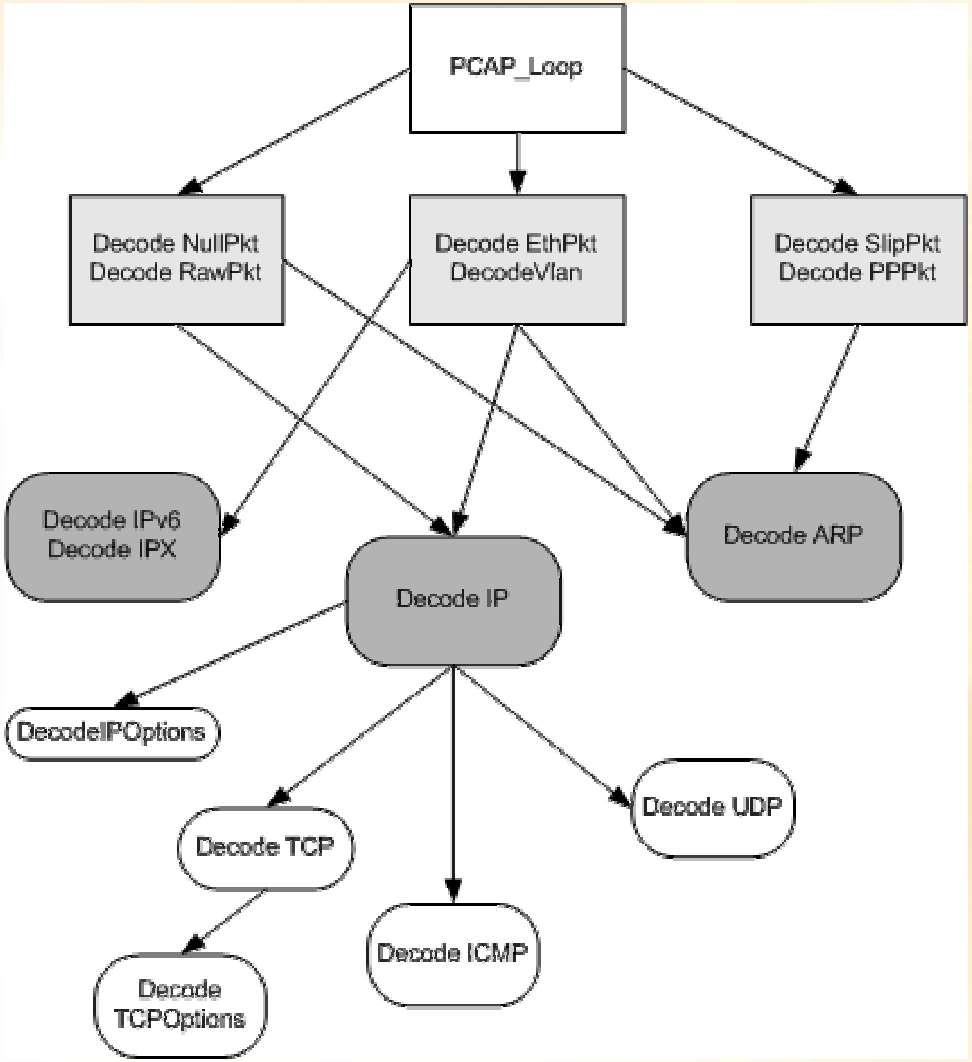

***Detection engine flow***

# SNORT – Alert/Logging module



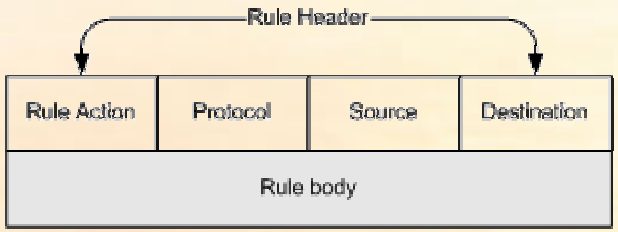

***Alert/logging module***

# SNORT – TCP/IP protocol suite




***TCP/IP protocol suite***

# SNORT – Rules Building




alert tcp !10.1.1.0/24 any -> 10.1.1.0/24 any (flags: SF; msg: “SYN-FIN Scan”;)

- Two sections to a rule
- rule header:

  alert tcp !10.1.1.0/24 any -> 10.1.1.0/24 any
- rule options:

(flags: SF; msg: “SYN-FIN Scan”;)

- Rule headers and options can be strung together in any combination

## SNORT – Rule header

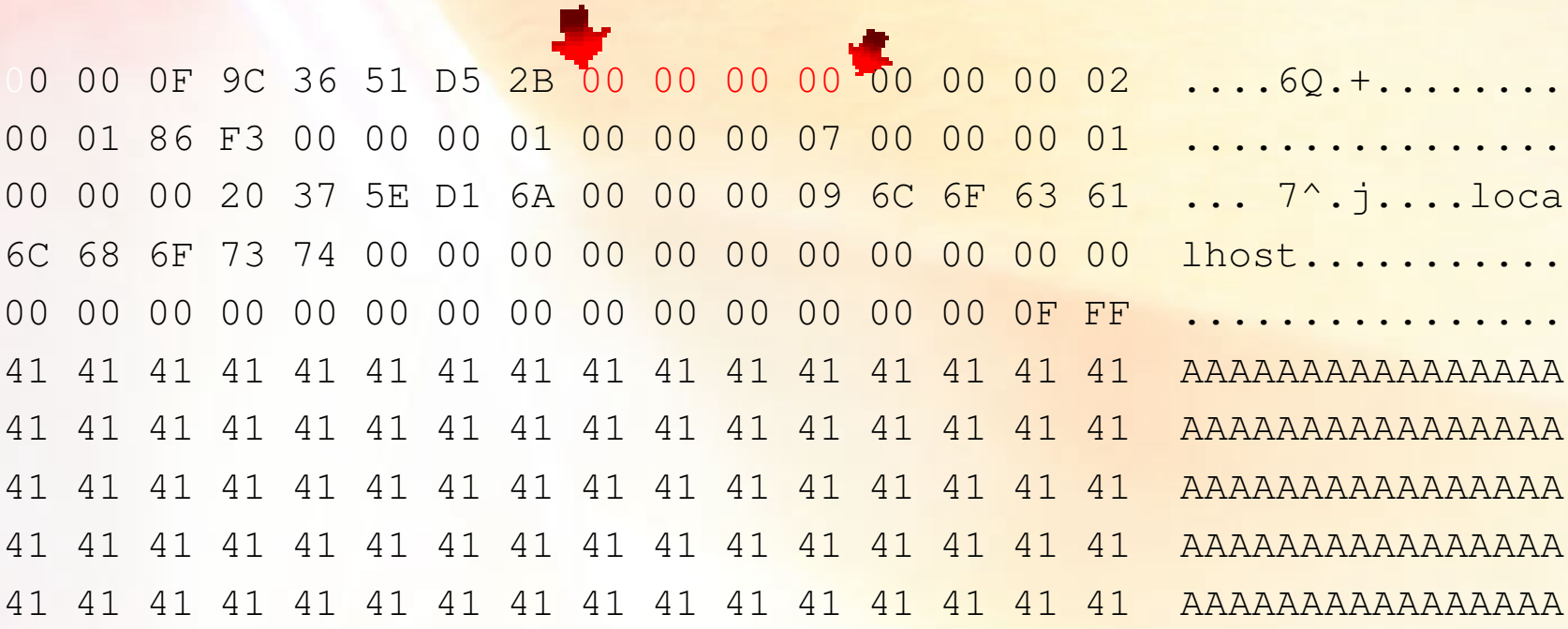
- IP addresses
  - negation, CIDR blocks
- TCP/UDP ports
  - negation, ranges, greater than/less than
- uni/bi-directional port/address consideration

# SNORT – Rule options

- Content
- Content offset
- Content depth
- Session recording
- ICMP type
- ICMP code
- Alternate log files
- IP TTL
- IP ID
- Fragment size
- TCP Flags
- TCP Ack number
- TCP Seq number
- Payload size

# SNORT – Rule options / Byte Jump

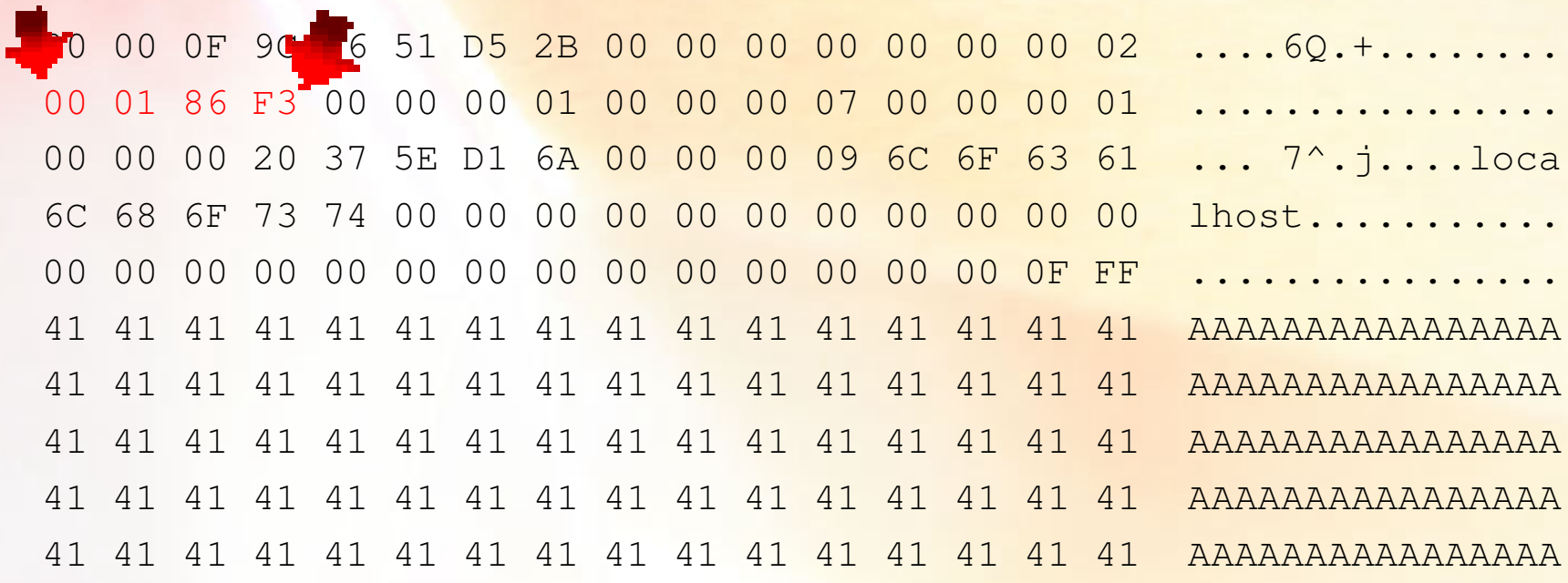
content:"|00 00 00 00|"; offset:8; depth:4; content:"|00 01 86 F3|"; offset:16; depth:4; content:"|00 00 00 07|"; distance:4; within:4; byte_jump:4,4,relative,align; byte_jump:4,4,relative,align; byte_test:4,>,128,0,relative;



```
00 00 0F 9C 36 51 D5 2B 00 00 00 00 00 00 00 02  ....6Q.+........
00 01 86 F3 00 00 00 01 00 00 00 07 00 00 00 01  ................
00 00 00 20 37 5E D1 6A 00 00 00 09 6C 6F 63 61  ... 7^.j....loca
6C 68 6F 73 74 00 00 00 00 00 00 00 00 00 00 00  lhost...........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 0F FF  ................
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
```

# SNORT – Rule options / Byte Jump

content:"|00 00 00 00|"; offset:8; depth:4; content:"|00 01 86 F3|";
offset:16; depth:4; content:"|00 00 00 07|"; distance:4; within:4;
byte_jump:4,4,relative,align; byte_jump:4,4,relative,align;
byte_[illegible]4,>,128,0,relative;



## SNORT – Uses for snort

- Standard packet sniffing NIDS
- Honeypot monitor

# References

- Snort website: www.snort.org
- Extending snort by Brian Caswell
- Martin Roesh – usenix conference
- Book: Syngres Snort 2.0
- Book: New Riders - Network Intrusion Detection
- And of course Google : )

Thank you!

Q & A