```
{
  "took" : 54,
  "timed_out" : false,
  "_shards" : {
    "total" : 5,
    "successful" : 5,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : 3173,
    "max_score" : 9.311229,
    "hits" : [
      {
        "_index" : "snort-logs",
        "_type" : "somedoctype",
        "_id" : "AV_a_-O0-7KAqxoxQs5N",
        "_score" : 9.311229,
        "_source" : {
          "content" : " 11971 (http_inspect) IIS UNICODE CODEPOINT
ENCODING Priority 3 11/10-101012.380506 10.2.198.24040606 "
        }
      },
      {
        "_index" : "snort-logs",
        "_type" : "somedoctype",
        "_id" : "AV_a_-UV-7KAqxoxQuDh",
        "_score" : 9.311229,
        "_source" : {
          "content" : " 11971 (http_inspect) IIS UNICODE CODEPOINT
ENCODING Priority 3 11/10-121148.939543 10.2.23.12750929 ->
154.241.88.20180 TCP "
        }
      },
      {
        "_index" : "snort-logs",
        "_type" : "somedoctype",
        "_id" : "AV_a_-U4-7KAqxoxQuQ-",
        "_score" : 8.375784,
        "_source" : {
          "content" : " 11971 (http_inspect) IIS UNICODE CODEPOINT
ENCODING Priority 3 11/10-123738.337645 10.2.23.19558492 ->
154.241.88.20180 TCP TTL61 TOS0x0 ID33449 IpLen20 DgmLen578 DF AP Seq
0xB15E26C7 Ack 0xF1368416 Win 0xB7 "
        }
      },
      {
        "_index" : "snort-logs",
        "_type" : "somedoctype",
        "_id" : "AV_a_-Wl-7KAqxoxQu0O",
        "_score" : 8.375784,
        "_source" : {
          "content" : " 11971 (http_inspect) IIS UNICODE CODEPOINT
ENCODING Priority 3 11/11-115814.973396 10.2.23.18337089 ->
154.241.88.20180 TCP TTL61 TOS0x0 ID47355 IpLen20 DgmLen490 DF AP Seq
0x69385547 Ack 0x4197BFAA Win 0xB7 "
        }
      },
      {
        "_index" : "snort-logs",
        "_type" : "somedoctype",
        "_id" : "AV_a_-WD-7KAqxoxQuo9",
        "_score" : 8.164521,
        "_source" : {
          "content" : " 11971 (http_inspect) IIS UNICODE CODEPOINT
ENCODING Priority 3 11/11-100427.293379 10.2.23.21251805 ->
154.241.88.20180 TCP TTL61 TOS0x0 ID17650 IpLen20 DgmLen376 DF AP Seq
0x5C2E84CC "
        }
      },
      {
        "_index" : "snort-logs",
        "_type" : "somedoctype",
        "_id" : "AV_a_-Am-7KAqxoxQpSL",
        "_score" : 7.4811697,
        "_source" : {
          "content" : " 11971 (http_inspect) IIS UNICODE CODEPOINT
ENCODING Priority 3 11/08-130509.369472 10.2.190.25445838 ->
154.241.88.20180 TCP TTL61 TOS0x0 ID37897 IpLen20 DgmLen1200 DF A Seq
0xE4701839 Ack 0x7E5857C6 Win 0xD8 TcpLen 32 TCP Options (3) => NOP NOP
TS 954149 77977951  "
        }
      },
      {
        "_index" : "snort-logs",
        "_type" : "somedoctype",
        "_id" : "AV_a_-EO-7KAqxoxQqCo",
        "_score" : 7.4811697,
        "_source" : {
          "content" : " 11971 (http_inspect) IIS UNICODE CODEPOINT
ENCODING Priority 3 11/08-133020.140308 10.2.199.23640807 ->
154.241.88.20180 TCP TTL61 TOS0x0 ID20823 IpLen20 DgmLen1200 DF A Seq
0xD4E203BF Ack 0x914F954 Win 0xD8 TcpLen 32 TCP Options (3) => NOP NOP TS
1333847 79496334  "
        }
      },
      {
        "_index" : "snort-logs",
        "_type" : "somedoctype",
        "_id" : "AV_a_-JQ-7KAqxoxQrpG",
        "_score" : 7.4811697,
        "_source" : {
          "content" : " 11971 (http_inspect) IIS UNICODE CODEPOINT
ENCODING Priority 3 11/10-095528.135941 10.2.198.24034292 ->
154.241.88.20180 TCP TTL61 TOS0x0 ID4621 IpLen20 DgmLen280 DF AP Seq
0x27EE9196 Ack 0x3DD45AB2 Win 0xB7 TcpLen 32 TCP Options (3) => NOP NOP
TS 361381 138650649  "
        }
      },
      {
        "_index" : "snort-logs",
        "_type" : "somedoctype",
        "_id" : "AV_a_-Kz-7KAqxoxQr88",
        "_score" : 7.4811697,
        "_source" : {
          "content" : " 11971 (http_inspect) IIS UNICODE CODEPOINT
ENCODING Priority 3 11/10-095604.972298 10.2.198.24034306 ->
154.241.88.20180 TCP TTL61 TOS0x0 ID55627 IpLen20 DgmLen462 DF AP Seq
0x49F07EF8 Ack 0x60C92C4C Win 0xB7 TcpLen 32 TCP Options (3) => NOP NOP
TS 370631 138687626  "
```

```
        }
      },
      {
        "_index" : "snort-logs",
        "_type" : "somedoctype",
        "_id" : "AV_a_-Lj-7KAqxoxQsKn",
        "_score" : 7.4811697,
        "_source" : {
          "content" : " 11971 (http_inspect) IIS UNICODE CODEPOINT
ENCODING Priority 3 11/10-095641.790116 10.2.198.24034839 ->
154.241.88.20180 TCP TTL61 TOS0x0 ID45167 IpLen20 DgmLen476 DF AP Seq
0x6D877B90 Ack 0x836D7857 Win 0xB7 TcpLen 32 TCP Options (3) => NOP NOP
TS 379884 138724619  "
        }
      }
    ]
  }
}
```