

**TUGAS**  
**KEAMANAN JARINGAN KOMPUTER**



**DISUSUN OLEH :**

**NAMA : INDAH SARI**

**NIM : 09011181320011**

**JURUSAN SISTEM KOMPUTER**

**FAKULTAS ILMU KOMPUTER**

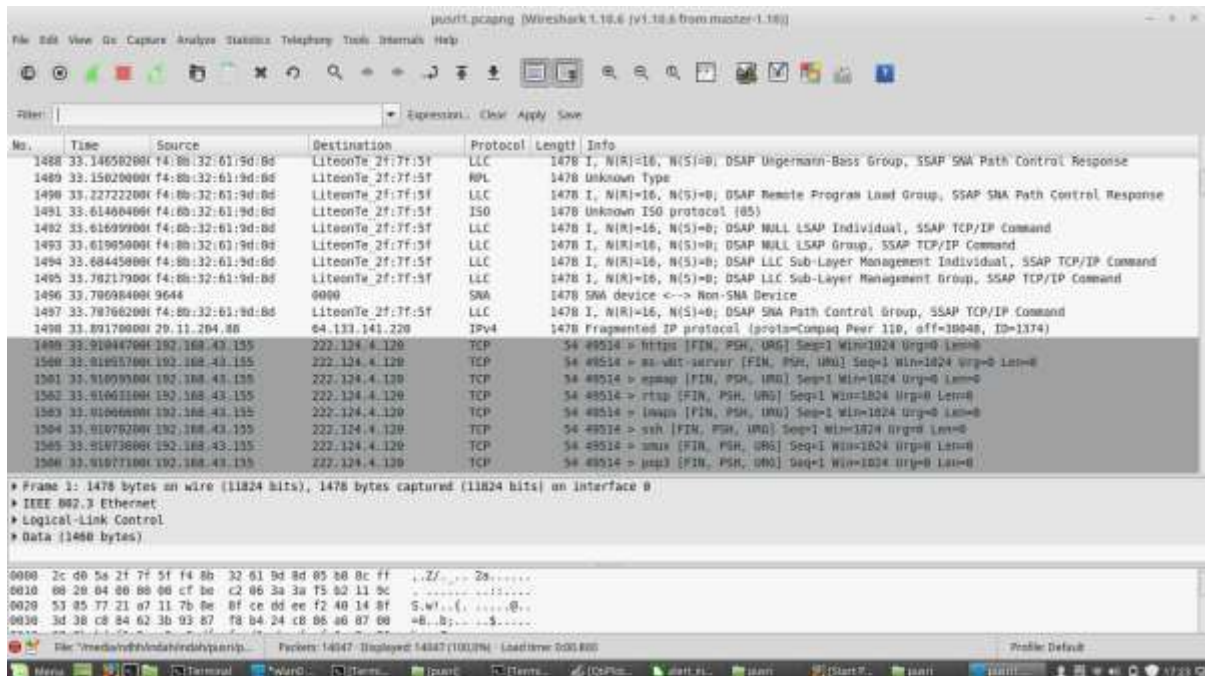
**UNIVERSITAS SRIWIJAYA**

**2017 – 2018**

TARGET : pusri.co.id

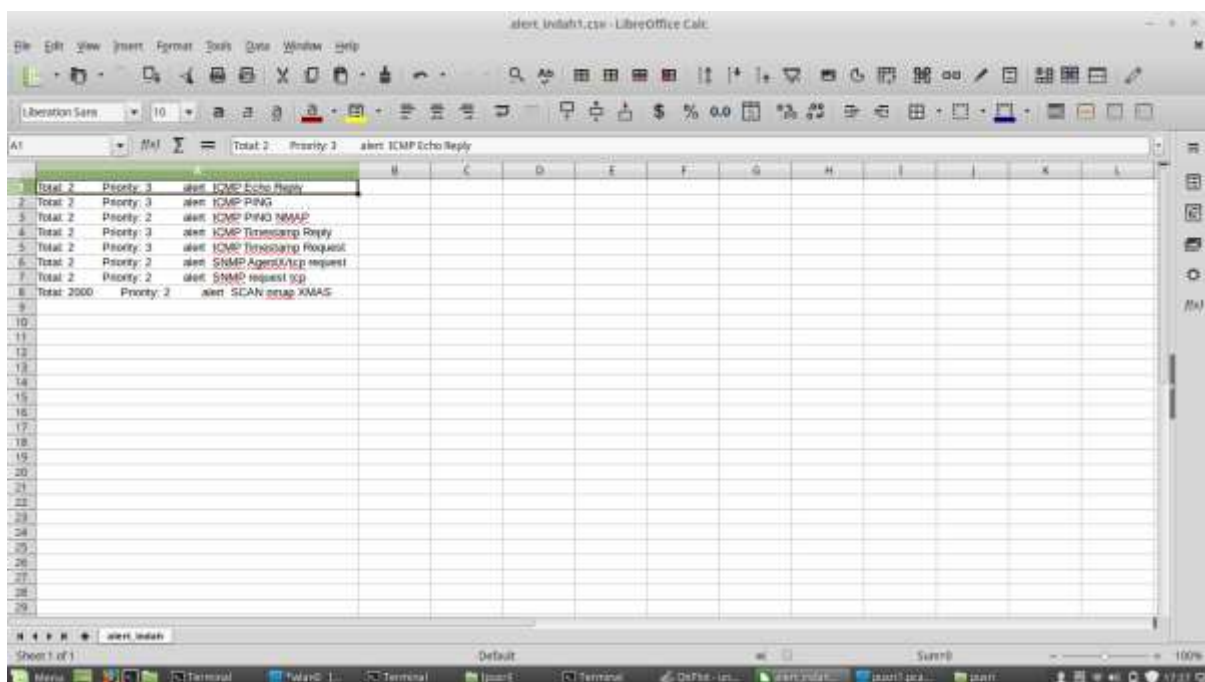
Tools yang digunakan Wireshark

Hasil scanning domain pusri.co.id yang dilakukan dengan menggunakan wireshark



Dari hasil scanning diatas menampilkan IP dari target, dimana IP yang digunakan pusri.co.id 222.124.4.120, dengan menggunakan protocol TCP

### HASIL DARI ALERT



## SCREENSHORT DARI COMPLE SNORT

Snort -A Fast -c /etc/snort/snort.conf -r .home/indah/indah/pusri/pusri.pcapng -l /var/log/snort

```
Terminal
File Edit View Search Terminal Help

--== Initialization Complete ==--

o" )~ -*) Snort! <*-
      Version 2.9.6.0 GRE (Build 47)
      By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-t
eam
      Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
      Copyright (C) 1998-2013 Sourcefire, Inc., et al.
      Using libpcap version 1.5.3
      Using PCRE version: 8.31 2012-07-06
      Using ZLIB version: 1.2.8

      Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.1 <Build 1>
      Preprocessor Object: SF_SDF Version 1.1 <Build 1>
      Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
      Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
      Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
      Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
      Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
      Preprocessor Object: SF_POP Version 1.0 <Build 1>
      Preprocessor Object: SF_SSH Version 1.1 <Build 3>
      Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
      Preprocessor Object: SF_DNS Version 1.1 <Build 4>
```

```
Terminal
File Edit View Search Terminal Help

      Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Commencing packet processing (pid=6000)

-----
Run time for packet processing was 1.23234 seconds
Snort processed 14047 packets.
Snort ran for 0 days 0 hours 0 minutes 1 seconds
  Pkts/sec:      14047
-----
Memory usage summary:
  Total non-mmapped bytes (arena):      37134336
  Bytes in mapped regions (hblkhd):     6868992
  Total allocated space (uordblks):     31561944
  Total free space (fordblks):          5572392
  Topmost releasable block (keepcost):  47408
-----
Packet I/O Totals:
  Received:      14047
  Analyzed:     14047 (100.000%)
  Dropped:       0 ( 0.000%)
  Filtered:      0 ( 0.000%)
  Outstanding:  0 ( 0.000%)
  Injected:      0
-----
Breakdown by protocol (includes rebuilt packets):
```

```

Terminal
File Edit View Search Terminal Help
UDP Discards: 0
Events: 972
Internal Events: 0
TCP Port Filter
Filtered: 0
Inspected: 0
Tracked: 2174
UDP Port Filter
Filtered: 0
Inspected: 26
Tracked: 2

=====

SMTP Preprocessor Statistics
Total sessions           : 0
Max concurrent sessions : 0

=====

dcerpc2 Preprocessor Statistics
Total sessions: 0

=====

SIP Preprocessor Statistics
Total sessions: 0

=====

```

Comple: phyton countalert.py alert alert\_indah.csv

```

ndhh@ndhh-Aspire-4250 /media/ndhh/indah/indah/pusri $ python countalert.py alert
alert_indah.csv
Total: 2      Priority: 3      alert ICMP Echo Reply
Total: 2      Priority: 3      alert ICMP PING
Total: 2      Priority: 2      alert ICMP PING NMAP
Total: 2      Priority: 3      alert ICMP Timestamp Reply
Total: 2      Priority: 3      alert ICMP Timestamp Request
Total: 2      Priority: 2      alert SNMP AgentX/tcp request
Total: 2      Priority: 2      alert SNMP request tcp
Total: 2000   Priority: 2      alert SCAN nmap XMAS
ndhh@ndhh-Aspire-4250 /media/ndhh/indah/indah/pusri $

```

### GRAP HASIL DARI ALERT

