https://www.sans.org/reading-room/whitepapers/protocols/analyzing-network-traffic-basic-linux-tools-34037

```
tcpdump -nn -r fake_av.pcap | wc -l
tcpdump -nn -r fake_av.pcap | head
```

```
[timestamp] [network protocol] [source IP].[source port] > [dest IP].[dest port]

tcpdump -nn -r fake_av.pcap | cut -f 3 -d " " | head

# Source IP address and port
tcpdump -nn -r fake_av.pcap 'tcp or udp' | cut -f 3 -d " " | head

# Source IP address
tcpdump -nn -r fake_av.pcap 'tcp or udp' | cut -f 3 -d " " | cut -f 1-4 -d "." | head

# Source IP address and sorted
tcpdump -nn -r fake_av.pcap 'tcp or udp'
```

```
| cut -f 3 -d " " | cut -f 1-4 -d "." |
sort | uniq | head

# Destination IP address
tcpdump -nn -r fake_av.pcap 'tcp or udp'
| cut -f 5 -d " " | cut -f 1-4 -d "." |
sort | uniq | head


# Destination IP address (top 10)
tcpdump -nn -r fake_av.pcap 'tcp or udp'
| cut -f 5 -d " " | cut -f 1-4 -d "." |
sort | uniq -c | sort -nr | head

# Destination IP address (SYN flag only
packets)
tcpdump -nn -r fake_av.pcap 'tcp[13]=2' |
cut -f 5 -d " " | sort | uniq -c | sort
-nr | head

# DNS traffic
tcpdump -nn -r fake_av.pcap 'port 53' |
head -5

# DNS traffic exclude common TLD
```

```
tcpdump -nn -r fake_av.pcap 'port 53' |
grep -Ev '(com|net|org|gov|mil|arpa)' |
cut -f 9 -d " " | head


# DNS traffic exclude common TLD, find
names only
tcpdump -nn -r fake_av.pcap 'port 53' |
grep -Ev '(com|net|org|gov|mil|arpa)' |
cut -f 8 -d " " | grep -E '[a-z]'

open virustotal and paste
http://puskovayaustanovka.ru

#  parse all pcap files in a folder to
tcpdump
cd /opt/samples/mta
for capfile  in $(ls *.pcap); do tcpdump
-nn -r $capfile 'port 53' | grep -Ev
'(com|net|org|gov|mil|arpa)' | cut -f 8
-d " " | grep -E '[a-z]'; done;

#  parse all pcap files in a folder to
tcpdump and find plain text passwords
for capfile  in $(ls *.pcap); do tcpdump
```

```
-nn -r $capfile  port http or port ftp or
port smtp or port imap or port pop3 or
port telnet -lA | egrep -i -B5
'pass=|pwd=|log=|login=|user=|username=|p
w=|passw=|passwd=
|password=|pass:|user:|username:|password
:|login:|pass |user '; done;
```