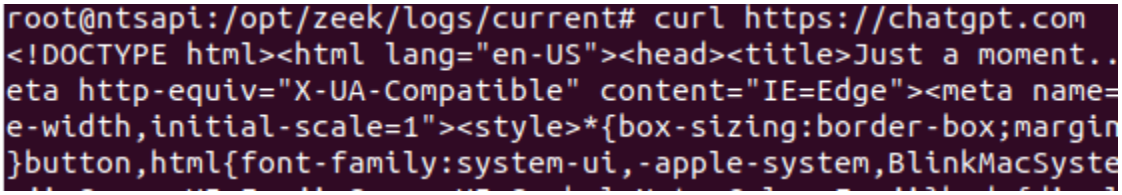
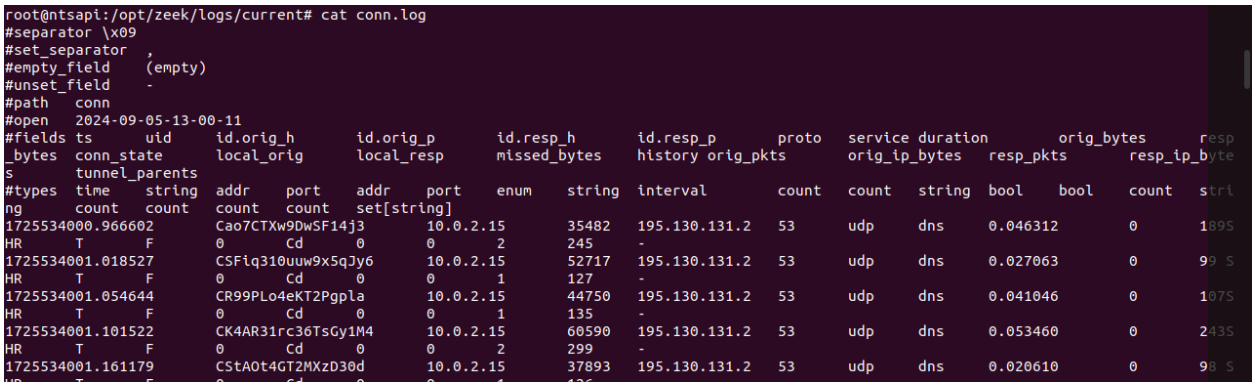
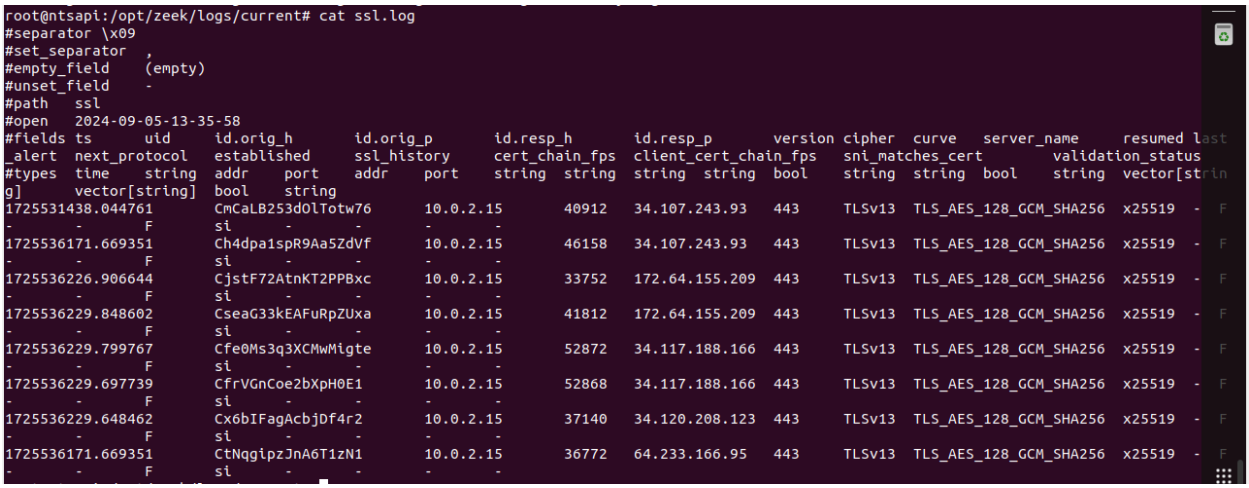
Zeek 2

1. Traffic Generation:Simulate different types of network traffic between the host and the VM. This can include:

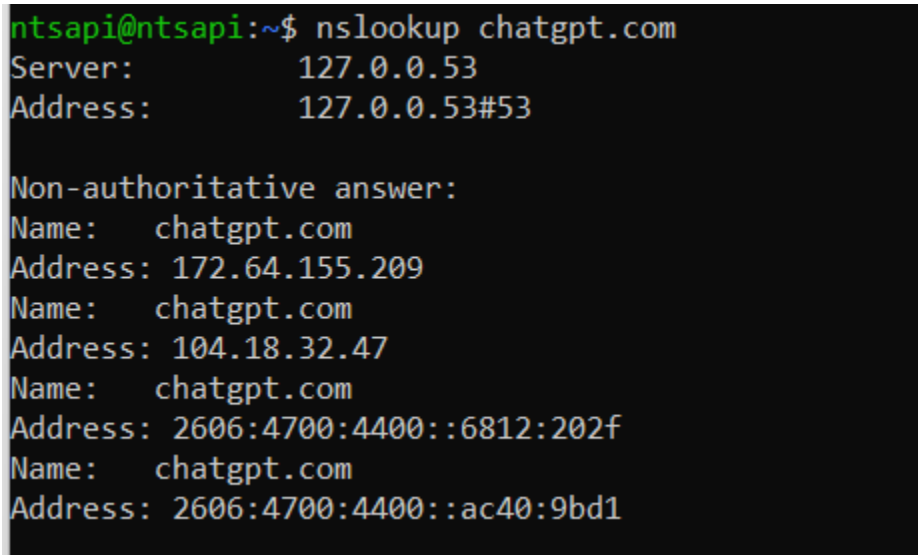
- Browsing websites (HTTP/HTTPS traffic)







- Performing DNS queries



```
root@ntsapi:/opt/zeek/logs/current# cat dns.log | grep chatgpt
1725536226.700447       C4a9dL3AmhR8CgtaR6      10.0.2.15       57142   195.130.130.2   53      udp     23271   -       chatgpt.com     -
-       -       -       0       NOERROR F       F       F       T       0       172.64.155.209,104.18.32.47     211.000000,211.000000 F
1725536226.700445       CMCgUX2lrIoHezgYAf      10.0.2.15       56512   195.130.130.2   53      udp     57607   -       chatgpt.com     -
-       -       -       0       NOERROR F       F       F       T       0       2606:4700:4400::ac40:9bd1,2606:4700:4400::6812:202f     3
00.000000,300.000000    F
1725536229.767338       CesVm81HEXPRjwEQKg      10.0.2.15       44792   195.130.130.2   53      udp     19598   -       ab.chatgpt.com-
-       -       -       0       NOERROR F       F       F       T       0       172.64.155.209,104.18.32.47     159.000000,159.000000 F
1725536229.775452       CAb6CR1Pnqc4OrrQvl      10.0.2.15       53956   195.130.130.2   53      udp     29568   -       ab.chatgpt.com-
-       -       -       0       NOERROR F       F       F       T       0       2606:4700:4400::6812:202f,2606:4700:4400::ac40:9bd1     1
25.000000,125.000000    F
```

```
ntsapi@ntsapi:~$ dig google.com

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43618
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             108     IN      A       64.233.167.100
google.com.             108     IN      A       64.233.167.138
google.com.             108     IN      A       64.233.167.101
google.com.             108     IN      A       64.233.167.102
google.com.             108     IN      A       64.233.167.139
google.com.             108     IN      A       64.233.167.113

;; Query time: 46 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Fri Sep 06 12:08:33 CEST 2024
;; MSG SIZE  rcvd: 135
```

```
root@ntsapi:/opt/zeek/logs/current# cat dns.log | grep google
1725534001.095690       CR99PLo4eKT2Pgpla       10.0.2.15       44750   195.130.131.2   53      udp     30195   -       82.221.107.34.i
n-addr.arpa     -       -       -       -       0       NOERROR F       F       F       T       0       82.221.107.34.bc.googleusercont
ent.com 120.000000      F
1725536171.669351       C66Cpx1bqahPcu3PD7      10.0.2.15       38384   195.130.131.2   53      udp     34440   -       safebrowsing.go
ogleapis.com    -       -       -       -       0       NOERROR F       F       F       T       0       64.233.166.95   264.000000      F
1725536171.669351       CFntIaeHmGLLY2rzl       10.0.2.15       44215   195.130.131.2   53      udp     5552    -       safebrowsing.go
ogleapis.com    -       -       -       -       0       NOERROR F       F       F       T       0       2a00:1450:400c:c09::5f  268.000
000     F
```

- Using SSH for remote connections

```
PS C:\Windows\system32> ssh ntsapi@192.168.0.132
The authenticity of host '192.168.0.132 (192.168.0.132)' can't be established.
ED25519 key fingerprint is SHA256:mT0qYHwHHVO29MbSoz28w59mBII3qvALAf7l3TlAfHU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.132' (ED25519) to the list of known hosts.
ntsapi@192.168.0.132's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.8.0-40-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

13 updates can be applied immediately.
3 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

1 additional security update can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

ntsapi@ntsapi:~$
```

```
root@ntsapi:/opt/zeek/logs/current# cat conn.log | zeek-cut id.orig_h id.resp_h proto service
10.0.2.15       195.130.131.2   udp     dns
10.0.2.15       195.130.131.2   udp     dns
10.0.2.15       195.130.131.2   udp     dns
10.0.2.15       195.130.131.2   udp     dns
10.0.2.15       195.130.131.2   udp     dns
10.0.2.15       195.130.131.2   udp     dns
10.0.2.15       195.130.131.2   udp     dns
10.0.2.15       195.130.131.2   udp     dns
10.0.2.15       195.130.131.2   udp     dns
10.0.2.15       195.130.131.2   udp     dns
10.0.2.15       195.130.131.2   udp     dns
10.0.2.15       34.107.221.82   tcp     -
10.0.2.15       34.107.221.82   tcp     -
10.0.2.15       195.130.131.2   udp     dns
10.0.2.15       195.130.131.2   udp     dns
10.0.2.15       195.130.131.2   udp     dns
10.0.2.15       195.130.131.2   udp     dns
10.0.2.15       195.130.131.2   udp     dns
10.0.2.15       195.130.131.2   udp     dns
```

2. Simulate Malicious Activities:Introduce some benign and malicious activities for Zeek to detect:

- Run a simple port scan from the host to the VM using nmap

```
root@ntsapi:/home/ntsapi# nmap -sS -p 1-1000 192.168.0.132
Starting Nmap 7.80 ( https://nmap.org ) at 2024-09-06 12:22 CEST
Nmap scan report for ntsapi (192.168.0.132)
Host is up (0.0000040s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

- Generate a suspicious HTTP request (e.g., accessing an HTTP only URL).

```
root@ntsapi:/opt/zeek/logs/current# wget "http://192.168.0.132/search?query=1%27%20OR%20%271%27%3D%271"
--2024-09-06 13:59:53--  http://192.168.0.132/search?query=1'%20OR%20'1'%3D'1
Connecting to 192.168.0.132:80... connected.
HTTP request sent, awaiting response... 404 Not Found
2024-09-06 13:59:53 ERROR 404: Not Found.

--2024-09-06 13:59:53--  http://192.168.0.132/search?query=1%27%20OR%20%271%27%3D%271
Reusing existing connection to 192.168.0.132:80.
HTTP request sent, awaiting response... 404 Not Found
2024-09-06 13:59:53 ERROR 404: Not Found.
```

3. Log Analysis: Analyze the logs generated by Zeek. Focus on the following log files:

- conn.log for connection summaries

Summarizing Connections by Source and Destination IP

```
root@ntsapi:/opt/zeek/logs/2024-09-09# cat conn.13:14:19-14:00:00.log | zeek-cut id.orig_h id.resp_h proto service conn_state orig_byte
s resp_bytes
2a02:1812:2d1d:8e00:281f:1c3b:646d:7fd3 2a07:de40:b250:131:10:151:131:30        tcp     -       OTH     0       218
2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2a02:26f0:3900:281::3148        tcp     -       S2      0       0
2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2a02:26f0:3900:281::3148        tcp     -       OTH     736     555
2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2603:1020:705:8::400    tcp     -       OTH     -       -
2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2a02:26f0:3900:189::2c1a        tcp     -       OTH     -       -
192.168.0.132   13.107.246.67   tcp     -       OTH     -       -
2a02:1812:2d1d:8e00:281f:1c3b:646d:7fd3 2620:1ec:bdf::67        tcp     -       RSTRH   0       0
2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2a00:1450:400c:c0c::be  tcp     -       SHR     -       -
```

```
root@ntsapi:/opt/zeek/logs/2024-09-09# cat conn.13:14:19-14:00:00.log | zeek-cut id.orig_h id.resp_h proto service conn_state orig_byte
s resp_bytes | wc -l
3793
```

Count of Connections per IP Pair

```
root@ntsapi:/opt/zeek/logs/2024-09-09# cat conn.13:14:19-14:00:00.log | zeek-cut id.orig_h id.resp_h | sort | uniq -c | sort -nr
   1292 2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2a02:1800:100::42:2
    751 2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2a02:1800:100::42:1
     88 192.168.0.132   195.130.130.2
     80 192.168.0.236   192.168.0.119
     55 192.168.0.119   192.168.0.236
     51 192.168.0.119   34.149.206.255
```

```
root@ntsapi:/opt/zeek/logs/2024-09-09# cat conn.13:14:19-14:00:00.log | zeek-cut id.orig_h id.resp_h | sort | uniq -c | sort -nr | wc -
l
416
```

Extracting only Successful connections

```
root@ntsapi:/opt/zeek/logs/2024-09-09# cat conn.13:14:19-14:00:00.log | zeek-cut id.orig_h id.resp_h proto service orig_bytes resp_byte
s conn_state | grep SF
2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2606:2800:133:206e:1315:22a5:2006:24fd  tcp     -       0       0       SF
2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2a02:26f0:9200::58dd:5321       tcp     http    155     187     SF
2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2a02:26f0:3900::1729:b229       tcp     ssl     486     4695    SF
2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2a02:26f0:3900::1729:b229       tcp     ssl     486     4726    SF
2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2a02:26f0:3900::1729:b229       tcp     ssl     5076    107712  SF
2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2a02:26f0:3900::1729:b229       tcp     ssl     486     4693    SF
2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2a02:26f0:3900::1729:b229       tcp     ssl     486     4713    SF
2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2a02:26f0:3900::1729:b229       tcp     ssl     486     4710    SF
2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2a02:26f0:3900::1729:b23a       tcp     ssl     2197    88375   SF
2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2620:1ec:12::239        tcp     -       4365    6968    SF
2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2a02:1800:100::42:1     udp     dns     143     302     SF
2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2a02:1800:100::42:1     udp     dns     153     260     SF
```

```
root@ntsapi:/opt/zeek/logs/2024-09-09# cat conn.13:14:19-14:00:00.log | zeek-cut id.orig_h id.resp_h proto service orig_bytes resp_byte
s conn_state | grep SF | wc -l
2643
```

- http.log for HTTP transactions

  Extract HTTP GET Requests

```
root@ntsapi:/opt/zeek/logs/2024-09-09# cat http.11:48:56-13:14:19.log | zeek-cut ts id.orig_h method host uri status_code | grep "GET"
1725875340.483605       2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 GET     ipv6.msftconnecttest.com        /connecttest.txt        200
1725875340.483605       192.168.0.119   GET     www.msftconnecttest.com /connecttest.txt        200
1725875340.483605       2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 GET     ipv6check-http.steamserver.net  /ipv6check      200
1725875340.483605       2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 GET     ocsp.digicert.com       /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTk45WiKd
PUwcMf8JgMC07ACYqr2AQUt2ui6qiqhIx56rTaD5iyxZV2ufQCEAsO+mmYSHCSpdZOwOelbvI=      200
1725875340.483605       192.168.0.119   GET     www.msftconnecttest.com /connecttest.txt        200
1725875340.483605       2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 GET     ipv6.msftconnecttest.com        /connecttest.txt        200
```

```
root@ntsapi:/opt/zeek/logs/2024-09-09# cat http.11:48:56-13:14:19.log | zeek-cut ts id.orig_h method host uri status_code | grep "GET"
| wc -l
29
```

  Filter by Host

```
root@ntsapi:/opt/zeek/logs/2024-09-09# cat http.11:48:56-13:14:19.log | zeek-cut ts id.orig_h method host uri status_code | grep "www.m
sftconnecttest.com"
1725875340.483605       192.168.0.119   GET     www.msftconnecttest.com /connecttest.txt        200
1725875340.483605       192.168.0.119   GET     www.msftconnecttest.com /connecttest.txt        200
```

  Filter by status Code

```
root@ntsapi:/opt/zeek/logs/2024-09-09# cat http.11:48:56-13:14:19.log | zeek-cut ts id.orig_h method host uri status_code | grep "200"
1725875340.483605       2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 GET     ipv6.msftconnecttest.com        /connecttest.txt        200
1725875340.483605       192.168.0.119   GET     www.msftconnecttest.com /connecttest.txt        200
1725875340.483605       2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 GET     ipv6check-http.steamserver.net  /ipv6check      200
1725875340.483605       2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 GET     ocsp.digicert.com       /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTk45WiKd
PUwcMf8JgMC07ACYqr2AQUt2ui6qiqhIx56rTaD5iyxZV2ufQCEAsO+mmYSHCSpdZOwOelbvI=      200
```

- dns.log for DNS queries

```
root@ntsapi:/opt/zeek/logs/2024-09-09# cat dns.11:48:56-13:14:19.log | zeek-cut query | sort | uniq
-
1.0.0.0.2.4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.1.2.0.a.2.ip6.arpa
1.8.b.5.5.0.2.5.b.a.4.8.3.e.1.e.0.0.e.8.d.1.d.2.2.1.8.1.2.0.a.2.ip6.arpa
2.0.0.0.2.4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.1.2.0.a.2.ip6.arpa
2.131.130.195.in-addr.arpa
3.d.f.7.d.6.4.6.b.3.c.1.f.1.8.2.0.0.e.8.d.1.d.2.2.1.8.1.2.0.a.2.ip6.arpa
accounts.google.com
activity-consumer.trafficmanager.net
activity.windows.com
```

```
root@ntsapi:/opt/zeek/logs/2024-09-09# cat dns.11:48:56-13:14:19.log | zeek-cut query
ntsapi.local
ntsapi.local
ntsapi.local
```

- ssl.log for SSL/TLS sessions

```
root@ntsapi:/opt/zeek/logs/2024-09-09# cat ssl.11:48:56-13:14:19.log | zeek-cut ts id.orig_h id.resp_h server_name version cipher
1725823213.425494       192.168.0.119   104.208.16.92   self.events.data.microsoft.com  TLSv13  TLS_AES_256_GCM_SHA384
1725821187.541891       192.168.0.119   155.133.248.39  ext2-ams1.steamserver.net       -       -
1725821063.007730       2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2a00:1450:400c:c0d::be  www.youtube.com -       -
1725822960.384811       2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2a01:b740:a41:e80::2:4  contacts.icloud.com     -       -
```

```
root@ntsapi:/opt/zeek/logs/2024-09-09# cat ssl.11:48:56-13:14:19.log | zeek-cut ts id.orig_h id.resp_h server_name version cipher | wc
-l
43
```

- weird.log for unusual activity

  Listing All Events

```
root@ntsapi:/opt/zeek/logs/2024-09-09# cat weird.11:48:56-13:14:19.log | zeek-cut ts id.orig_h id.resp_h name addl
1725875340.919288       fe80::410c:23ab:5718:fccc       ff02::1:2       bad_UDP_checksum        -
1725875343.127657       2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2603:1030:c02:2::284    truncated_tcp_payload   -
1725875343.772895       192.168.0.132   151.101.10.49   active_connection_reuse -
1725875344.034610       2a02:1812:2d1d:8e00:281f:1c3b:646d:7fd3 2a04:4e42:2::561        active_connection_reuse -
1725875344.034611       192.168.0.132   91.189.91.49    active_connection_reuse -
1725875344.235722       192.168.0.132   185.125.188.58  active_connection_reuse -
1725875345.683708       2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2620:1ec:12::239        truncated_tcp_payload   -
```

  Filtering for Truncated TCP Payloads: This command isolates instances of truncated TCP payloads, which can indicate network issues or potential attacks.

```
root@ntsapi:/opt/zeek/logs/2024-09-09# cat weird.11:48:56-13:14:19.log | zeek-cut ts id.orig_h id.resp_h name addl | grep "truncated_tc
p_payload"
1725875343.127657       2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2603:1030:c02:2::284    truncated_tcp_payload   -
1725875345.683708       2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2620:1ec:12::239        truncated_tcp_payload   -
1725875345.962427       2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2603:1030:c02:2::284    truncated_tcp_payload   -
1725875346.650016       2a02:1812:2d1d:8e00:281f:1c3b:646d:7fd3 2a04:4e42:2::561        truncated_tcp_payload   -
root@ntsapi:/opt/zeek/logs/2024-09-09#
```

Analyzing Bad Udp Checksum Events: Look for patterns or frequent occurrences of bad udp checksums, which might signal network problems or missconfigurations.

```
root@ntsapi:/opt/zeek/logs/2024-09-09# cat weird.11:48:56-13:14:19.log | zeek-cut ts id.orig_h id.resp_h name addl
| grep "bad_UDP_checksum"
1725875340.919288       fe80::410c:23ab:5718:fccc       ff02::1:2       bad_UDP_checksum        -
1725875343.127657       2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2603:1030:c02:2::284    truncated_tcp_payload   -
1725875343.772895       192.168.0.132   151.101.10.49   active_connection_reuse -
1725875344.034610       2a02:1812:2d1d:8e00:281f:1c3b:646d:7fd3 2a04:4e42:2::561        active_connection_reuse -
1725875344.034611       192.168.0.132   91.189.91.49    active_connection_reuse -
1725875344.235722       192.168.0.132   185.125.188.58  active_connection_reuse -
1725875345.683708       2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2620:1ec:12::239        truncated_tcp_payload   -
1725875345.871532       2a02:1812:2d1d:8e00:281f:1c3b:646d:7fd3 2a04:4e42:2::561        active_connection_reuse -
1725875345.962427       2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2603:1030:c02:2::284    truncated_tcp_payload   -
1725875346.045528       192.168.0.132   185.125.188.58  above_hole_data_without_any_acks        -
1725875346.601607       2a02:1812:2d1d:8e00:281f:1c3b:646d:7fd3 2a04:4e42:2::561        above_hole_data_without_any_acks        -
1725875346.650016       2a02:1812:2d1d:8e00:281f:1c3b:646d:7fd3 2a04:4e42:2::561        truncated_tcp_payload   -
1725875347.058608       2a02:1812:2d1d:8e00:281f:1c3b:646d:7fd3 2620:1ec:bdf::67        active_connection_reuse -
1725875347.067760       2a02:1812:2d1d:8e00:281f:1c3b:646d:7fd3 2620:2d:4000:1::101     active_connection_reuse -
1725875347.104886       2a02:1812:2d1d:8e00:281f:1c3b:646d:7fd3 2620:2d:4002:1::102     active_connection_reuse -
1725875347.146643       192.168.0.132   185.125.188.54  active_connection_reuse -
1725875347.174967       2a02:1812:2d1d:8e00:281f:1c3b:646d:7fd3 2a07:de40:b250:131:10:151:131:30        active_connection_reuse -
1725875347.239332       2a02:1812:2d1d:8e00:281f:1c3b:646d:7fd3 2620:2d:4000:1::101     above_hole_data_without_any_acks        -
1725875347.325982       2a02:1812:2d1d:8e00:281f:1c3b:646d:7fd3 2620:2d:4002:1::102     above_hole_data_without_any_acks        -
1725875347.730888       2a02:1812:2d1d:8e00:e1e3:84ab:5205:5b81 2a02:26f0:3900:281::3148        data_before_established -
1725875348.005329       2a02:1812:2d1d:8e00:281f:1c3b:646d:7fd3 2620:2d:4000:1::2e      active_connection_reuse -
1725875351.361170       2a02:1812:2d1d:8e00:281f:1c3b:646d:7fd3 2620:2d:4000:1::2e      above_hole_data_without_any_acks        -
1725875351.426031       2a02:1812:2d1d:8e00:281f:1c3b:646d:7fd3 2620:1ec:bdf::67        data_after_reset        -
1725875351.426031       2a02:1812:2d1d:8e00:281f:1c3b:646d:7fd3 2620:1ec:bdf::67        above_hole_data_without_any_acks        -
bash: syntax error near unexpected token `|'
root@ntsapi:/opt/zeek/logs/2024-09-09#
```