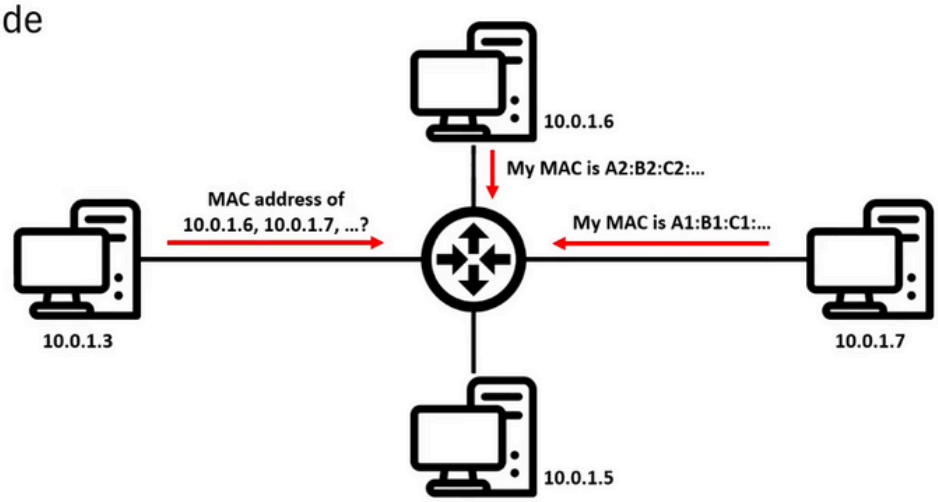
Table of contents

"Master in Cybersecurity" designed by Chema Alonso

Sniffing types – Techniques

- Promiscuous mode
- DNS Spoofing
- ARP Spoofing
- DHCP Sniffing



Sniffing tools

Source: https://www.wireshark.org/

Source: https://www.tcpdump.org/

Sniffing tools – Wireshark

- Wireshark is a graphical application to capture live network traffic or analyze captured traffic from a file in a visual way.
- You can inspect individual packets, see detailed information about protocols used, and apply filters to focus on specific traffic types.

Source: https://gitlab.com/wireshark/wireshark

Sniffing tools – TShark

- Tshark is a command-line version of Wireshark.
- Offers the same functionalities as Wireshark for capturing and analyzing traffic, but through text-based commands.
- Useful for scripting or automation purposes

```
$> sudo apt install tshark

rawshark    mergecap    editcap    text2pcap
```

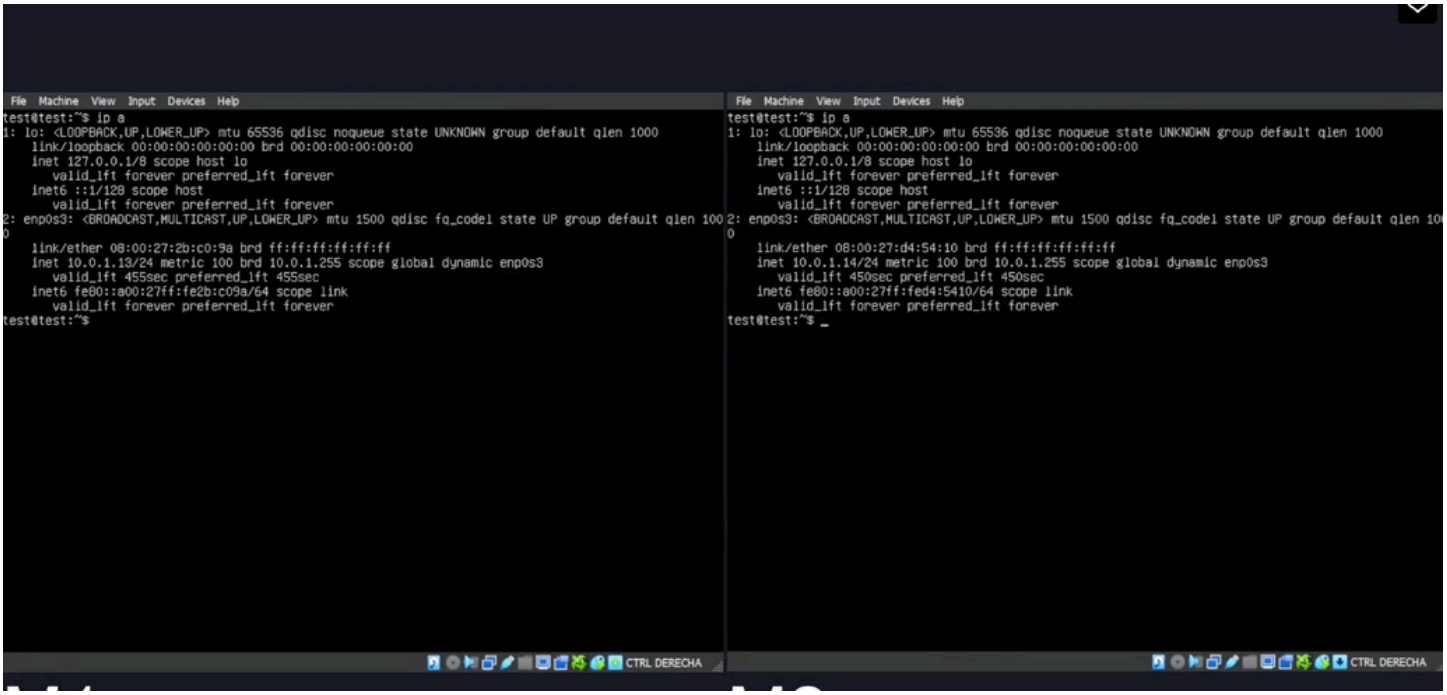
Sniffing tools – TCPdump

- TCPdump is a command-line tool for capturing network traffic on Unix-based systems.
- Useful for capturing traffic on remote machines or when a graphical interface isn't available.

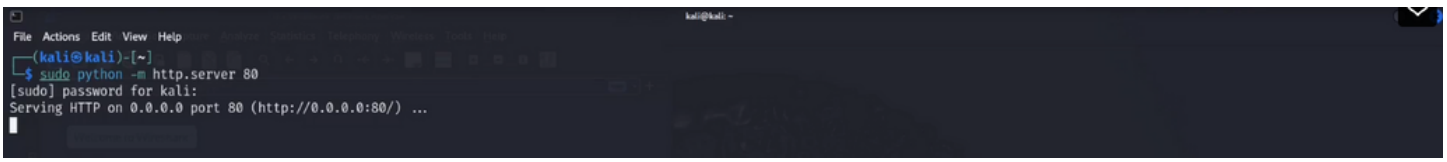
Source: https://www.tcpdump.org/

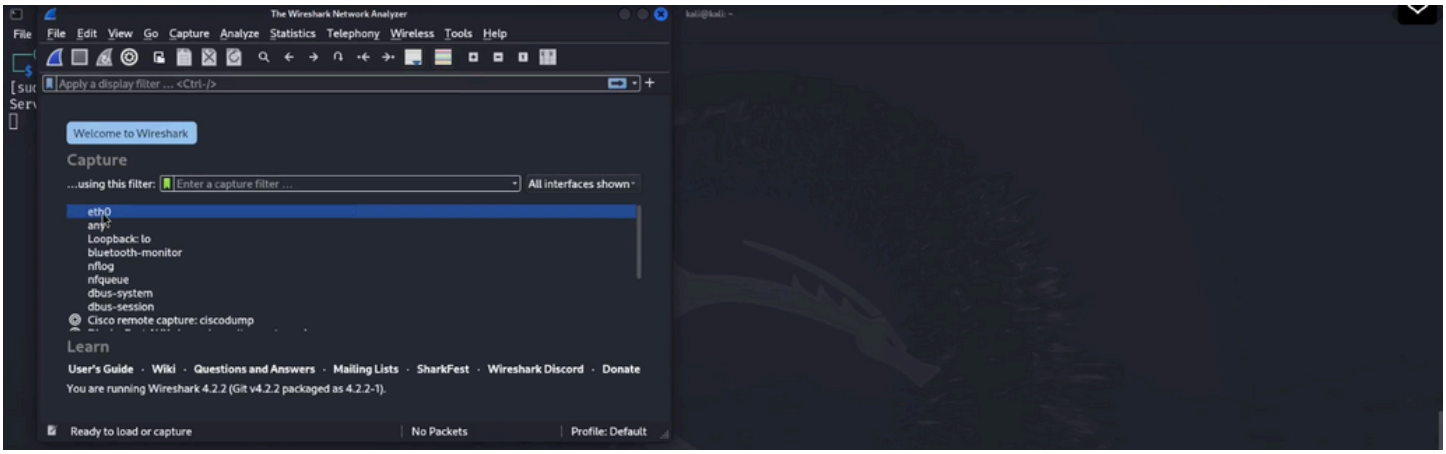
Presentación de las maquinas del laboratorio, con las cuales vamos a simular tráfico para utilizar las herramientas mencionadas, Wireshark, Tshark y TCPDump:

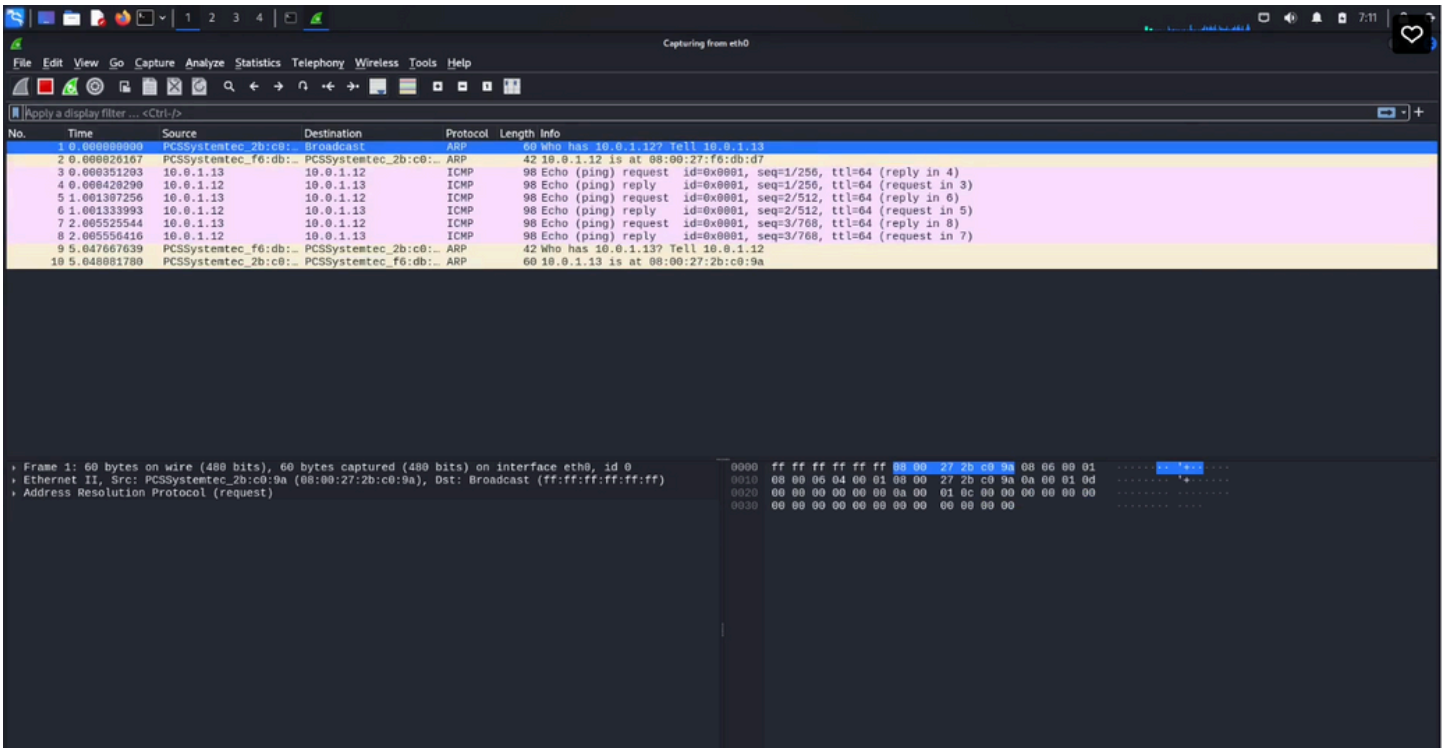

File Actions Edit View Help
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.1.12 netmask 255.255.255.0 broadcast 10.0.1.255
inet6 fe80::8d28:f520:a582:55be prefixlen 64 scopeid 0x20<link>
ether 08:00:27:f6:db:d7 txqueuelen 1000 (Ethernet)
RX packets 46 bytes 15072 (14.7 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 43 bytes 6150 (6.0 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 4 bytes 240 (240.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 4 bytes 240 (240.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(kali㉿kali)-[~]
$

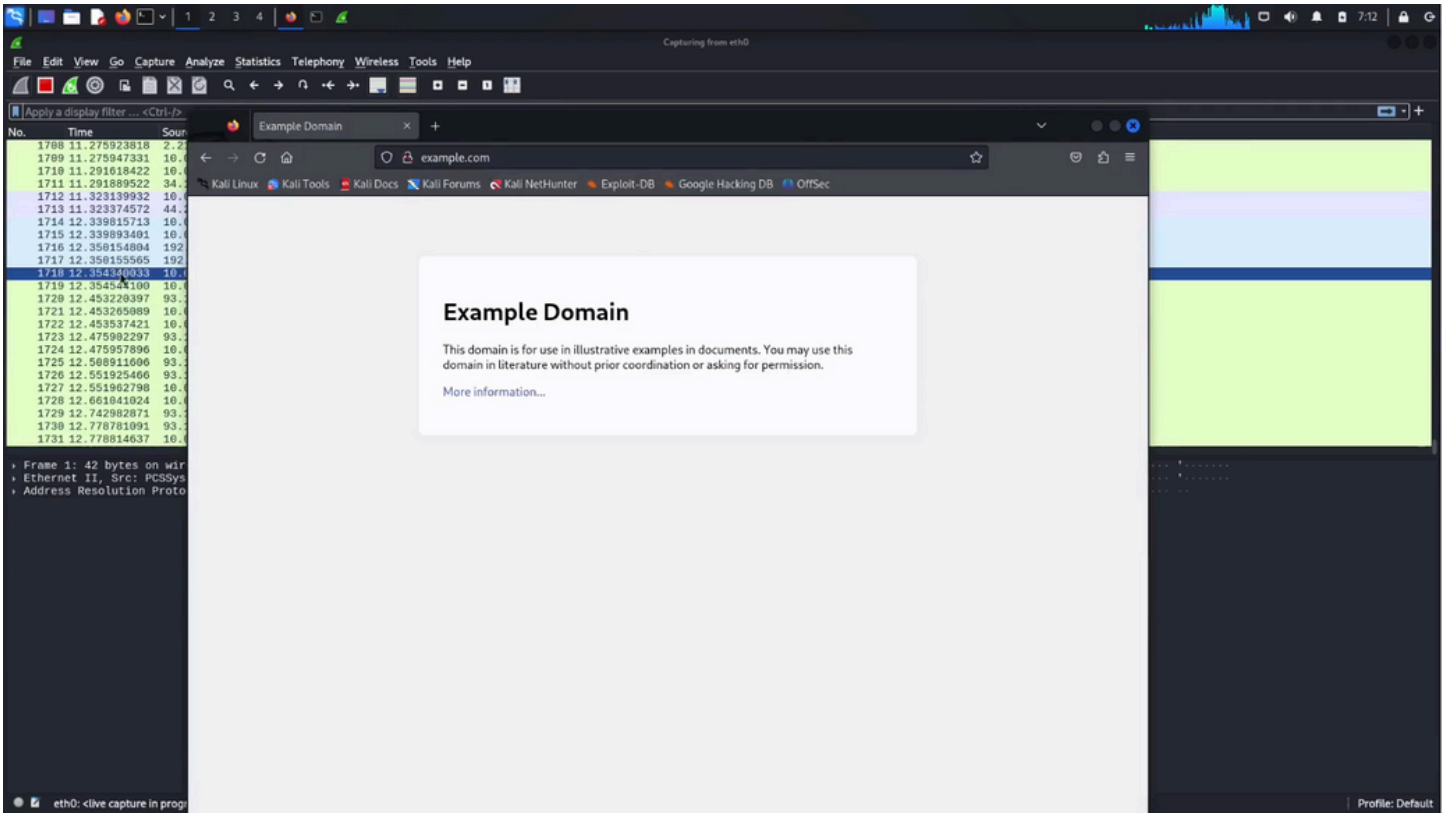

File Machine View Input Devices Help
test@test:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:2b:c0:9a brd ff:ff:ff:ff:ff:ff
inet 10.0.1.13/24 metric 100 brd 10.0.1.255 scope global dynamic enp0s3
valid_lft 455sec preferred_lft 455sec
inet6 fe80::a00:27ff:fe2b:c09a/64 scope link
valid_lft forever preferred_lft forever
test@test:~$
CTRL DERECHA
File Machine View Input Devices Help
test@test:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:d4:54:10 brd ff:ff:ff:ff:ff:ff
inet 10.0.1.14/24 metric 100 brd 10.0.1.255 scope global dynamic enp0s3
valid_lft 450sec preferred_lft 450sec
inet6 fe80::a00:27ff:fed4:5410/64 scope link
valid_lft forever preferred_lft forever
test@test:~$
CTRL DERECHA

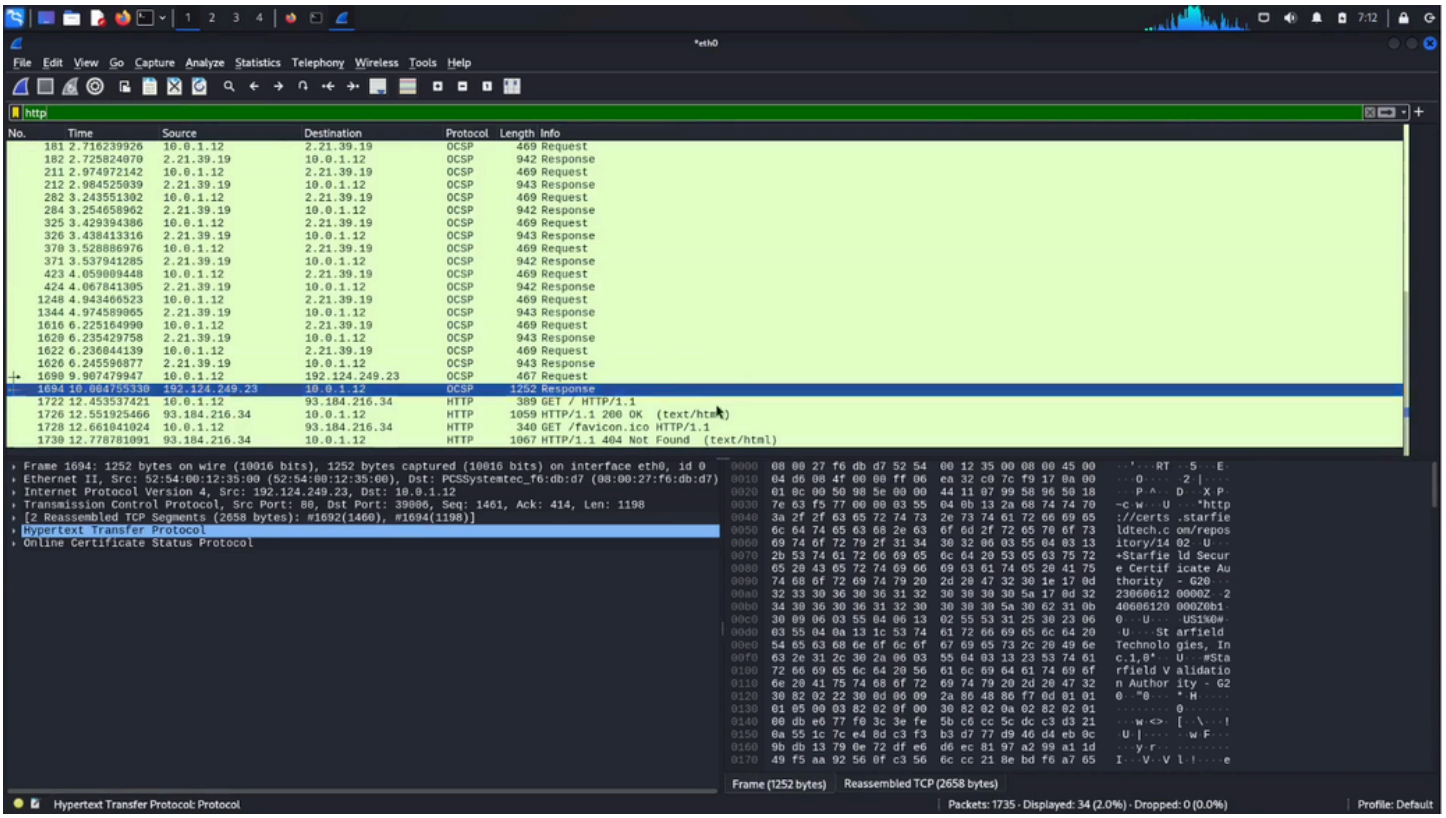
Wireshark:


File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo python -m http.server 80
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...

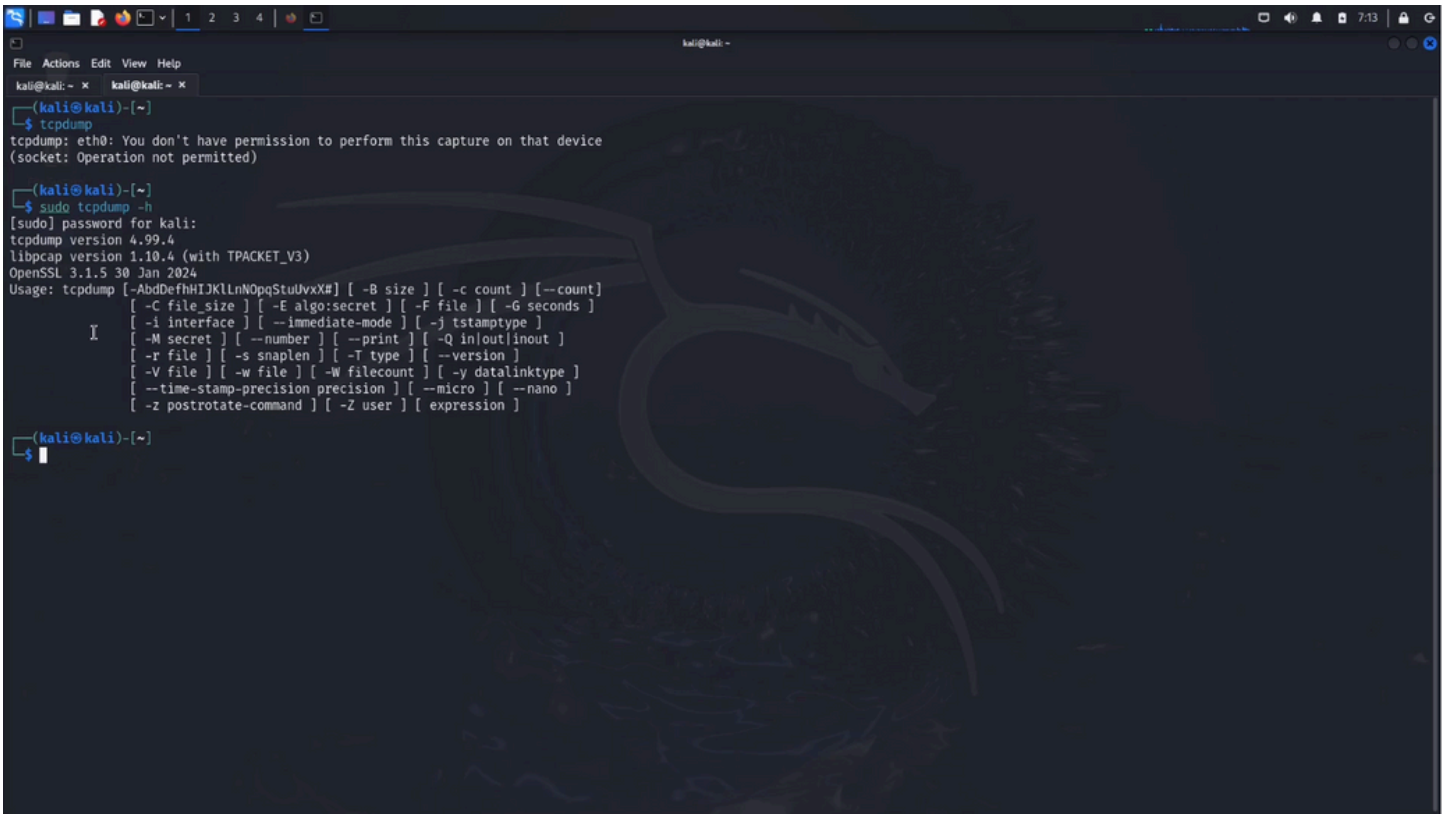

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.2.2 (Git v4.2.2 packaged as 4.2.2-1).
Ready to load or capture
No Packets
Profile: Default

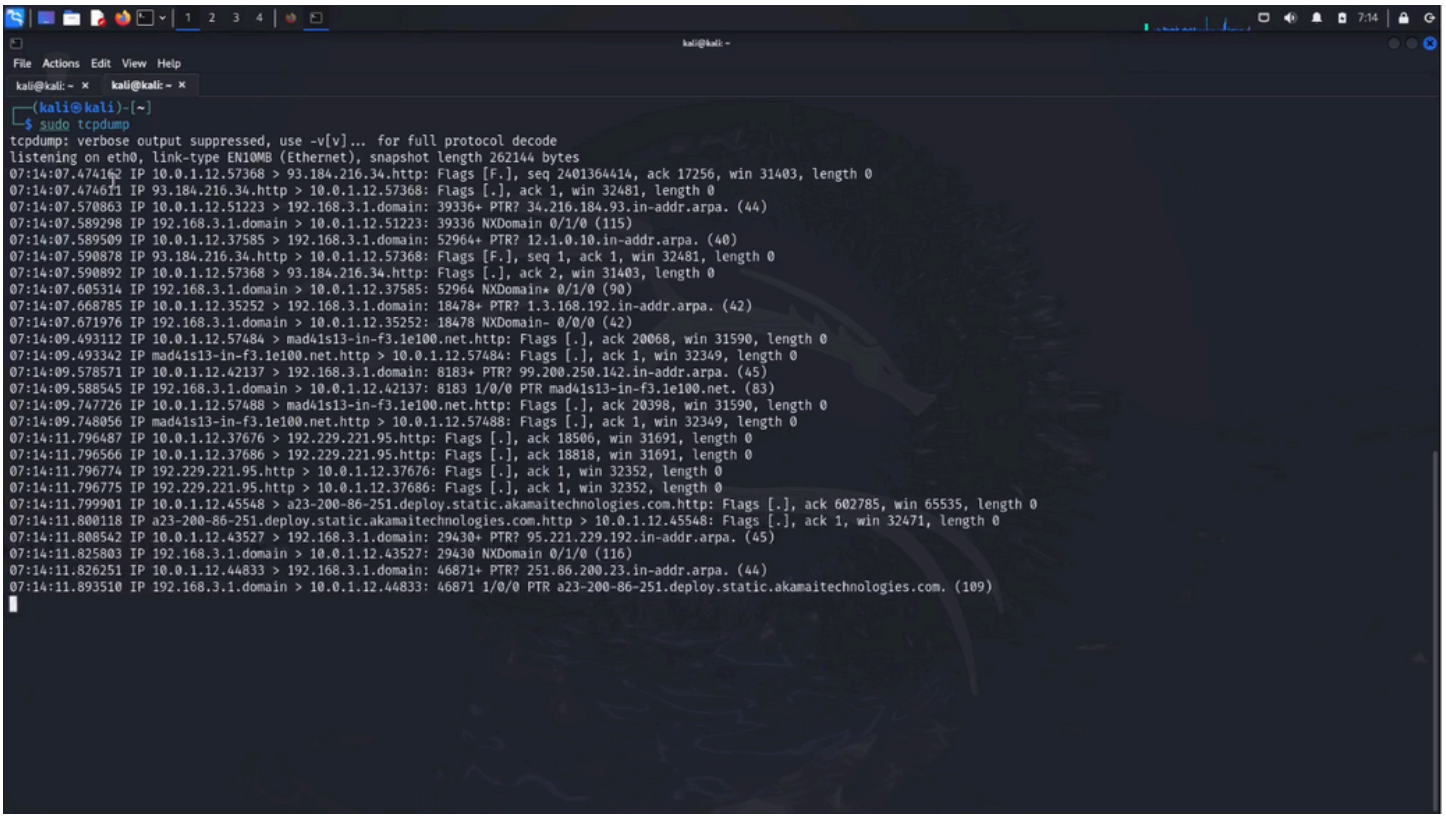

Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 PCSSystemtec_2b:c0:... Broadcast ARP 60 Who has 10.0.1.12? Tell 10.0.1.13
2 0.000026167 PCSSystemtec_f6:db:... PCSSystemtec_2b:c0:... ARP 42 10.0.1.12 is at 08:00:27:f6:db:d7
3 0.000351203 10.0.1.13 10.0.1.12 ICMP 98 Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 4)
4 0.000420290 10.0.1.12 10.0.1.13 ICMP 98 Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 3)
5 1.001307256 10.0.1.13 10.0.1.12 ICMP 98 Echo (ping) request id=0x0001, seq=2/512, ttl=64 (reply in 6)
6 1.001333993 10.0.1.12 10.0.1.13 ICMP 98 Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request in 5)
7 2.005525544 10.0.1.13 10.0.1.12 ICMP 98 Echo (ping) request id=0x0001, seq=3/768, ttl=64 (reply in 8)
8 2.005556416 10.0.1.12 10.0.1.13 ICMP 98 Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request in 7)
9 5.047667639 PCSSystemtec_f6:db:... PCSSystemtec_2b:c0:... ARP 42 Who has 10.0.1.13? Tell 10.0.1.12
10 5.048081780 PCSSystemtec_2b:c0:... PCSSystemtec_f6:db:... ARP 60 10.0.1.13 is at 08:00:27:2b:c0:9a
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_2b:c0:9a (08:00:27:2b:c0:9a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 08 00 27 2b c0 9a 08 06 00 01
0010 08 00 06 04 00 01 08 00 27 2b c0 9a 0a 00 01 0d
0020 00 00 00 00 00 00 0a 00 01 0c 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00

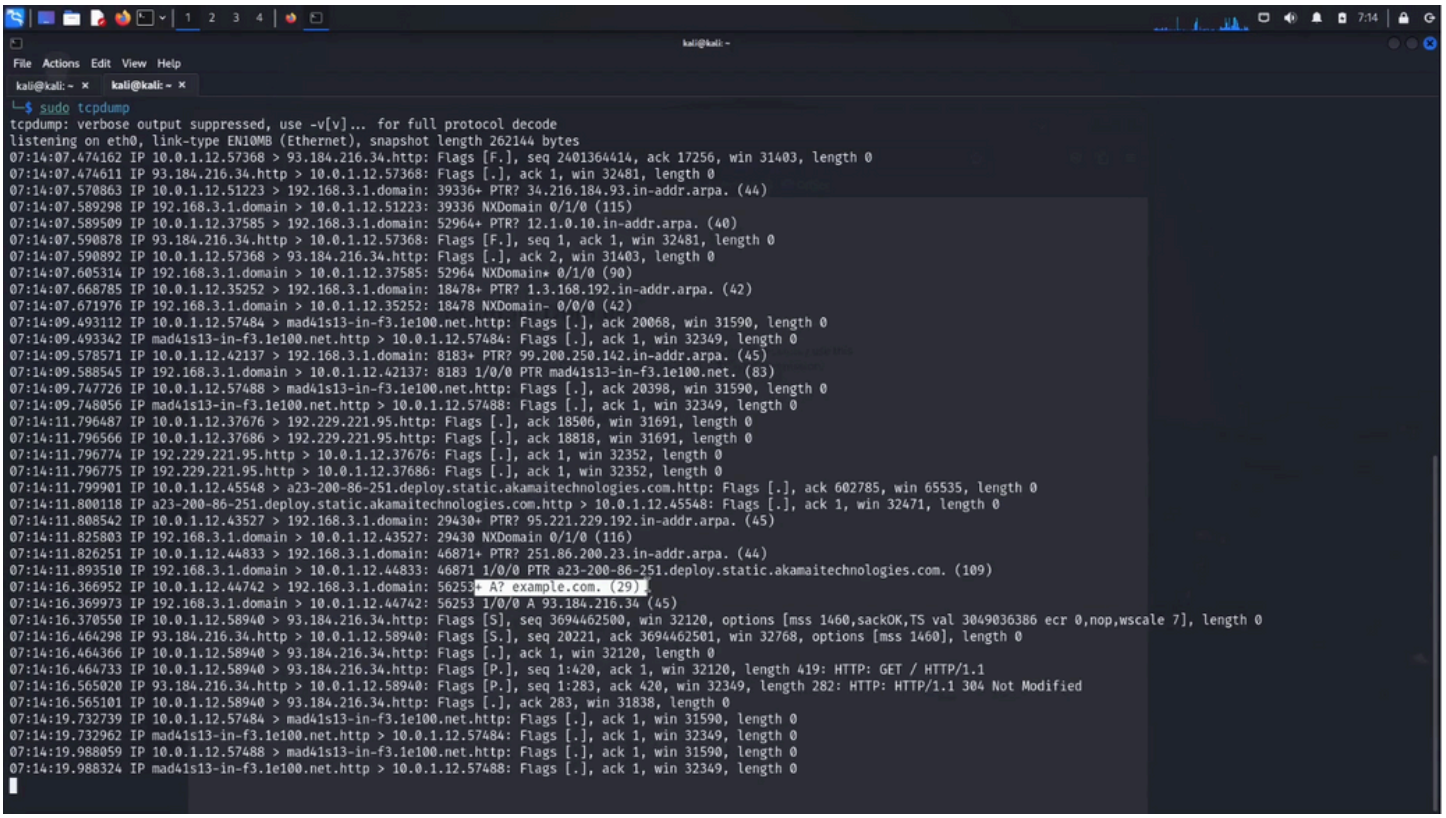

Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time
1708 11.275923818
1709 11.275947331
1710 11.291618422
1711 11.291889522
1712 11.323139932
1713 11.323374572
1714 12.339815713
1715 12.339893401
1716 12.350154804
1717 12.350155565
1718 12.354340033
1719 12.354544100
1720 12.453220397
1721 12.453265089
1722 12.453537421
1723 12.475902297
1724 12.475957896
1725 12.508911606
1726 12.551925466
1727 12.551962798
1728 12.661041024
1729 12.742982871
1730 12.778781091
1731 12.778814637
Example Domain
example.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Example Domain
This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission.
More information...
Profile: Default


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
181 2.716239926 10.0.1.12 2.21.39.19 OCSP 469 Request
182 2.725824070 2.21.39.19 10.0.1.12 OCSP 942 Response
211 2.974972142 10.0.1.12 2.21.39.19 OCSP 469 Request
212 2.984525039 2.21.39.19 10.0.1.12 OCSP 943 Response
282 3.243551302 10.0.1.12 2.21.39.19 OCSP 469 Request
284 3.254658962 2.21.39.19 10.0.1.12 OCSP 942 Response
325 3.429394386 10.0.1.12 2.21.39.19 OCSP 469 Request
326 3.438413316 2.21.39.19 10.0.1.12 OCSP 943 Response
370 3.528886976 10.0.1.12 2.21.39.19 OCSP 469 Request
371 3.537941285 2.21.39.19 10.0.1.12 OCSP 942 Response
423 4.059009448 10.0.1.12 2.21.39.19 OCSP 469 Request
424 4.067841305 2.21.39.19 10.0.1.12 OCSP 942 Response
1248 4.943466523 10.0.1.12 2.21.39.19 OCSP 469 Request
1344 4.974589065 2.21.39.19 10.0.1.12 OCSP 943 Response
1616 6.225164990 10.0.1.12 2.21.39.19 OCSP 469 Request
1620 6.235429758 2.21.39.19 10.0.1.12 OCSP 943 Response
1622 6.236844139 10.0.1.12 2.21.39.19 OCSP 469 Request
1626 6.245590877 2.21.39.19 10.0.1.12 OCSP 943 Response
1690 9.907479947 10.0.1.12 192.124.249.23 OCSP 467 Request
1694 10.004755330 192.124.249.23 10.0.1.12 OCSP 1252 Response
1722 12.453537421 10.0.1.12 93.184.216.34 HTTP 389 GET / HTTP/1.1
1726 12.551925466 93.184.216.34 10.0.1.12 HTTP 1059 HTTP/1.1 200 OK (text/html)
1728 12.661041024 10.0.1.12 93.184.216.34 HTTP 340 GET /favicon.ico HTTP/1.1
1730 12.778781091 93.184.216.34 10.0.1.12 HTTP 1067 HTTP/1.1 404 Not Found (text/html)
Frame 1694: 1252 bytes on wire (10016 bits), 1252 bytes captured (10016 bits) on interface eth0, id 0
Ethernet II, Src: 52:54:00:12:35:00 (52:54:00:12:35:00), Dst: PCSSystemtec_f6:db:d7 (08:00:27:f6:db:d7)
Internet Protocol Version 4, Src: 192.124.249.23, Dst: 10.0.1.12
Transmission Control Protocol, Src Port: 80, Dst Port: 39006, Seq: 1461, Ack: 414, Len: 1198
[2 Reassembled TCP Segments (2658 bytes): #1692(1460), #1694(1198)]
Hypertext Transfer Protocol
Online Certificate Status Protocol
Frame (1252 bytes)
Reassembled TCP (2658 bytes)
Hypertext Transfer Protocol: Protocol
Packets: 1735 · Displayed: 34 (2.0%) · Dropped: 0 (0.0%)
Profile: Default

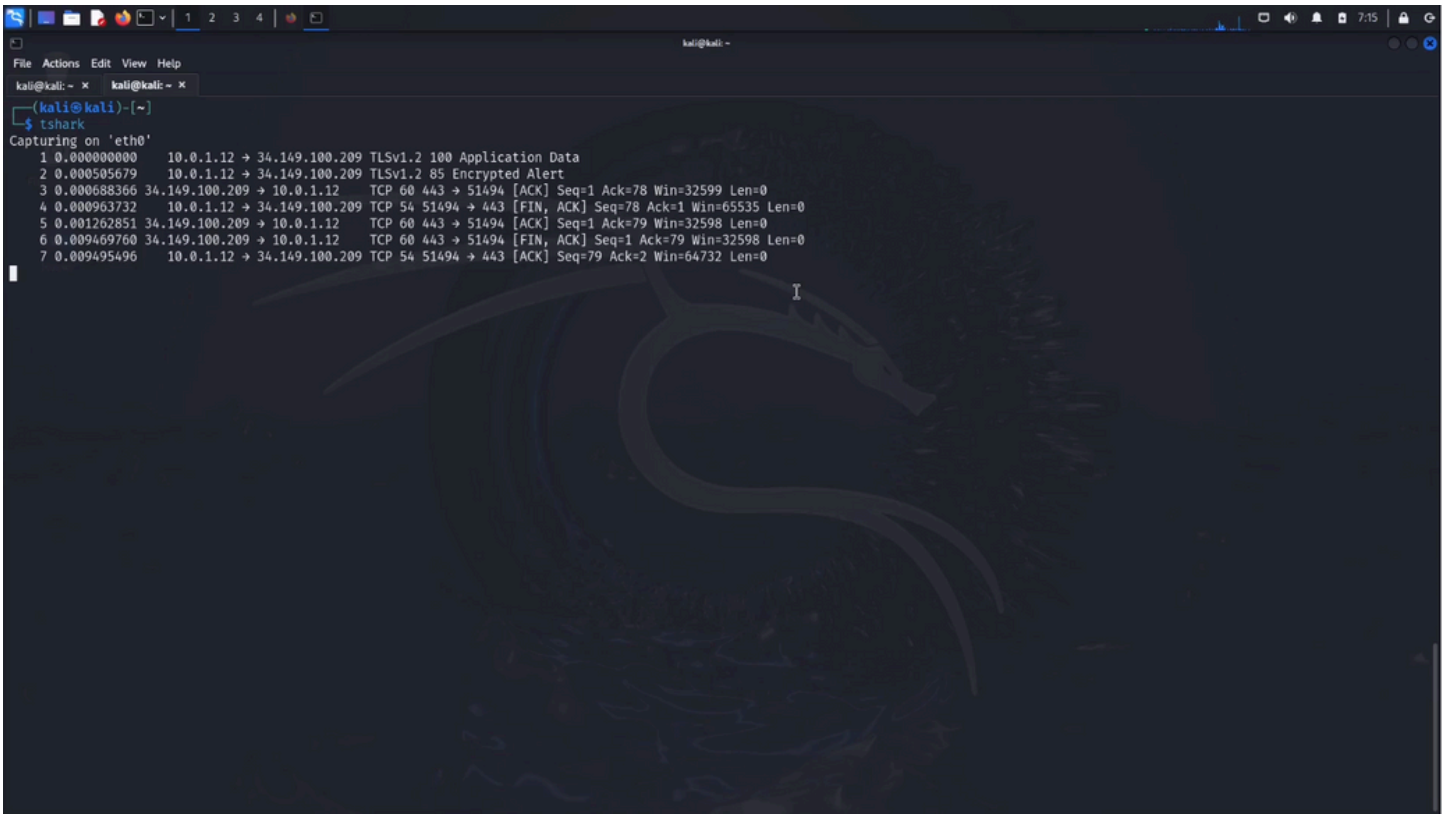
TCPDump:


kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
(kali㉿kali)-[~]
$ tcpdump
tcpdump: eth0: You don't have permission to perform this capture on that device
(socket: Operation not permitted)
(kali㉿kali)-[~]
$ sudo tcpdump -h
[sudo] password for kali:
tcpdump version 4.99.4
libpcap version 1.10.4 (with TPACKET_V3)
OpenSSL 3.1.5 30 Jan 2024
Usage: tcpdump [-AbdDefhHIJKlLnNOpqStuUvxX#] [-B size] [-c count] [--count]
[-C file_size] [-E algo:secret] [-F file] [-G seconds]
[-i interface] [--immediate-mode] [-j tstamptype]
[-M secret] [--number] [--print] [-Q in|out|inout]
[-r file] [-s snaplen] [-T type] [--version]
[-V file] [-w file] [-W filecount] [-y datalinktype]
[--time-stamp-precision precision] [--micro] [--nano]
[-z postrotate-command] [-Z user] [expression]
(kali㉿kali)-[~]
$

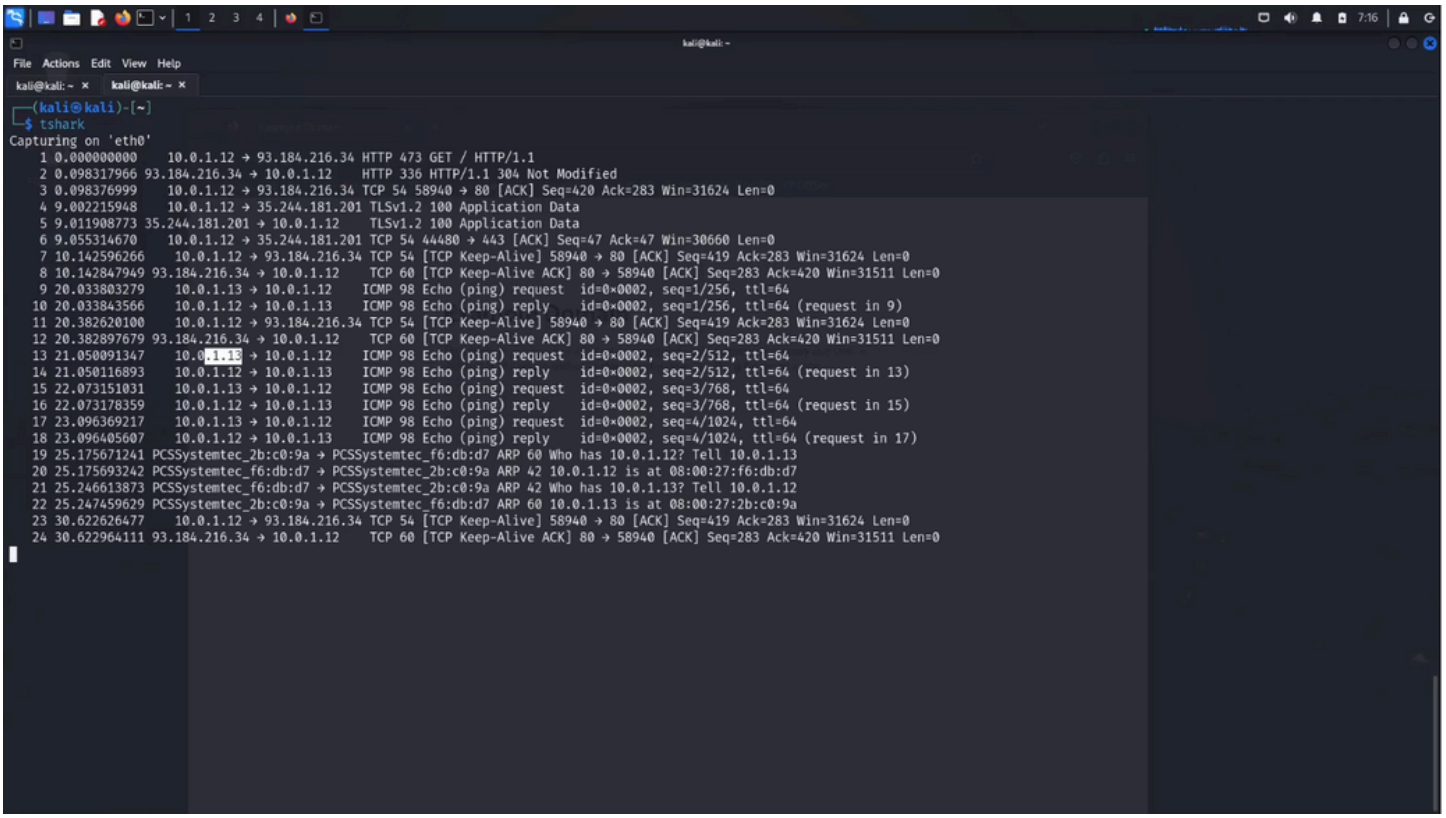

File Actions Edit View Help
kali@kali: ~
kali@kali: ~
$ sudo tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
07:14:07.474162 IP 10.0.1.12.57368 > 93.184.216.34.http: Flags [F.], seq 2401364414, ack 17256, win 31403, length 0
07:14:07.474611 IP 93.184.216.34.http > 10.0.1.12.57368: Flags [.], ack 1, win 32481, length 0
07:14:07.570863 IP 10.0.1.12.51223 > 192.168.3.1.domain: 39336+ PTR? 34.216.184.93.in-addr.arpa. (44)
07:14:07.589298 IP 192.168.3.1.domain > 10.0.1.12.51223: 39336 NXDomain 0/1/0 (115)
07:14:07.589509 IP 10.0.1.12.37585 > 192.168.3.1.domain: 52964+ PTR? 12.1.0.10.in-addr.arpa. (40)
07:14:07.590878 IP 93.184.216.34.http > 10.0.1.12.57368: Flags [F.], seq 1, ack 1, win 32481, length 0
07:14:07.590892 IP 10.0.1.12.57368 > 93.184.216.34.http: Flags [.], ack 2, win 31403, length 0
07:14:07.605314 IP 192.168.3.1.domain > 10.0.1.12.37585: 52964 NXDomain* 0/1/0 (90)
07:14:07.668785 IP 10.0.1.12.35252 > 192.168.3.1.domain: 18478+ PTR? 1.3.168.192.in-addr.arpa. (42)
07:14:07.671976 IP 192.168.3.1.domain > 10.0.1.12.35252: 18478 NXDomain- 0/0/0 (42)
07:14:09.493112 IP 10.0.1.12.57484 > mad41s13-in-f3.1e100.net.http: Flags [.], ack 20068, win 31590, length 0
07:14:09.493342 IP mad41s13-in-f3.1e100.net.http > 10.0.1.12.57484: Flags [.], ack 1, win 32349, length 0
07:14:09.578571 IP 10.0.1.12.42137 > 192.168.3.1.domain: 8183+ PTR? 99.200.250.142.in-addr.arpa. (45)
07:14:09.588545 IP 192.168.3.1.domain > 10.0.1.12.42137: 8183 1/0/0 PTR mad41s13-in-f3.1e100.net. (83)
07:14:09.747726 IP 10.0.1.12.57488 > mad41s13-in-f3.1e100.net.http: Flags [.], ack 20398, win 31590, length 0
07:14:09.748056 IP mad41s13-in-f3.1e100.net.http > 10.0.1.12.57488: Flags [.], ack 1, win 32349, length 0
07:14:11.796487 IP 10.0.1.12.37676 > 192.229.221.95.http: Flags [.], ack 18506, win 31691, length 0
07:14:11.796566 IP 10.0.1.12.37686 > 192.229.221.95.http: Flags [.], ack 18818, win 31691, length 0
07:14:11.796774 IP 192.229.221.95.http > 10.0.1.12.37676: Flags [.], ack 1, win 32352, length 0
07:14:11.796775 IP 192.229.221.95.http > 10.0.1.12.37686: Flags [.], ack 1, win 32352, length 0
07:14:11.799901 IP 10.0.1.12.45548 > a23-200-86-251.deploy.static.akamaitechnologies.com.http: Flags [.], ack 602785, win 65535, length 0
07:14:11.800118 IP a23-200-86-251.deploy.static.akamaitechnologies.com.http > 10.0.1.12.45548: Flags [.], ack 1, win 32471, length 0
07:14:11.808542 IP 10.0.1.12.43527 > 192.168.3.1.domain: 29430+ PTR? 95.221.229.192.in-addr.arpa. (45)
07:14:11.825803 IP 192.168.3.1.domain > 10.0.1.12.43527: 29430 NXDomain 0/1/0 (116)
07:14:11.826251 IP 10.0.1.12.44833 > 192.168.3.1.domain: 46871+ PTR? 251.86.200.23.in-addr.arpa. (44)
07:14:11.893510 IP 192.168.3.1.domain > 10.0.1.12.44833: 46871 1/0/0 PTR a23-200-86-251.deploy.static.akamaitechnologies.com. (109)

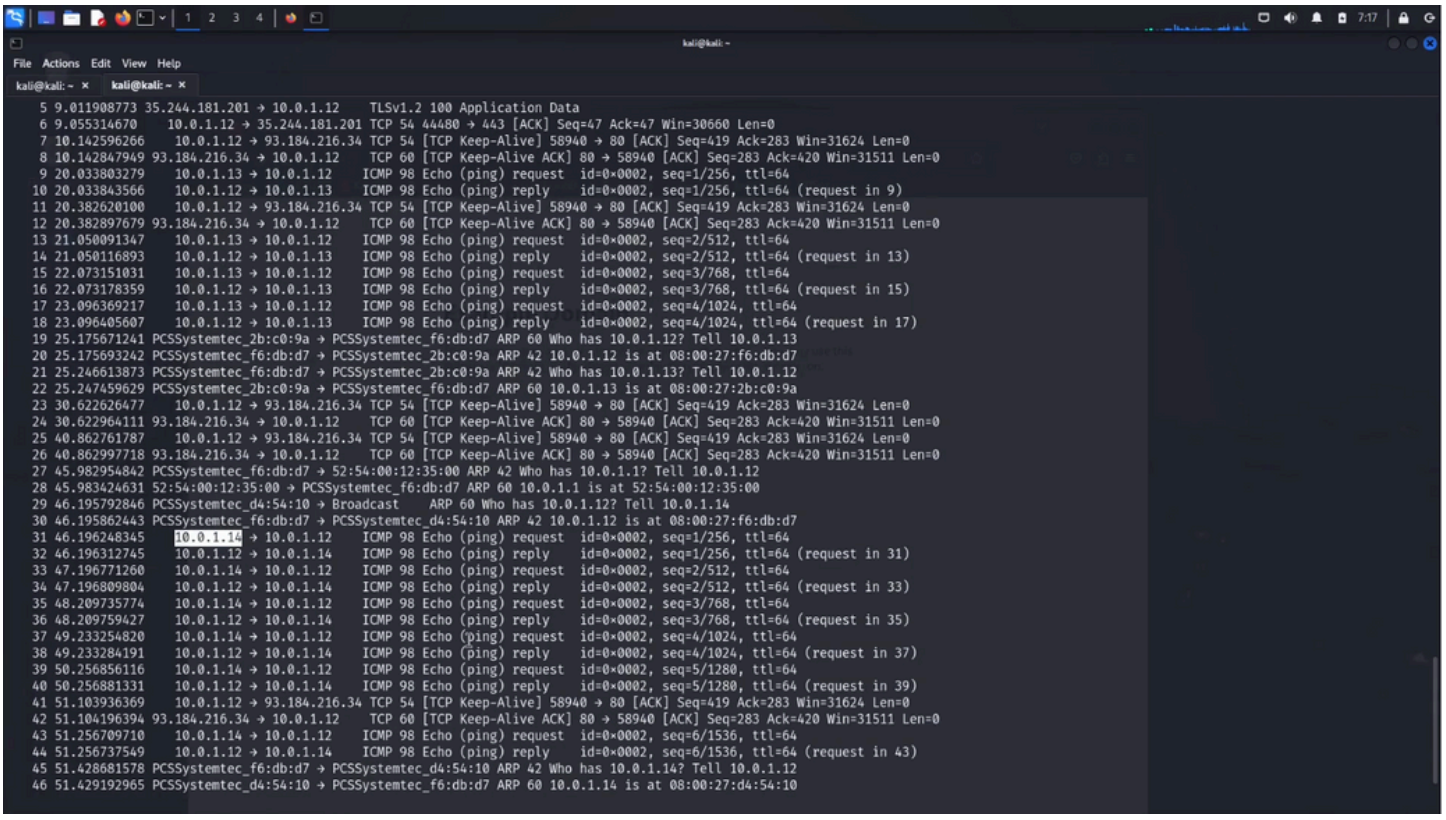

File Actions Edit View Help
kali@kali: ~
kali@kali: ~
$ sudo tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
07:14:07.474162 IP 10.0.1.12.57368 > 93.184.216.34.http: Flags [F.], seq 2401364414, ack 17256, win 31403, length 0
07:14:07.474611 IP 93.184.216.34.http > 10.0.1.12.57368: Flags [.], ack 1, win 32481, length 0
07:14:07.570863 IP 10.0.1.12.51223 > 192.168.3.1.domain: 39336+ PTR? 34.216.184.93.in-addr.arpa. (44)
07:14:07.589298 IP 192.168.3.1.domain > 10.0.1.12.51223: 39336 NXDomain 0/1/0 (115)
07:14:07.589509 IP 10.0.1.12.37585 > 192.168.3.1.domain: 52964+ PTR? 12.1.0.10.in-addr.arpa. (40)
07:14:07.590878 IP 93.184.216.34.http > 10.0.1.12.57368: Flags [F.], seq 1, ack 1, win 32481, length 0
07:14:07.590892 IP 10.0.1.12.57368 > 93.184.216.34.http: Flags [.], ack 2, win 31403, length 0
07:14:07.605314 IP 192.168.3.1.domain > 10.0.1.12.37585: 52964 NXDomain* 0/1/0 (90)
07:14:07.668785 IP 10.0.1.12.35252 > 192.168.3.1.domain: 18478+ PTR? 1.3.168.192.in-addr.arpa. (42)
07:14:07.671976 IP 192.168.3.1.domain > 10.0.1.12.35252: 18478 NXDomain- 0/0/0 (42)
07:14:09.493112 IP 10.0.1.12.57484 > mad41s13-in-f3.1e100.net.http: Flags [.], ack 20068, win 31590, length 0
07:14:09.493342 IP mad41s13-in-f3.1e100.net.http > 10.0.1.12.57484: Flags [.], ack 1, win 32349, length 0
07:14:09.578571 IP 10.0.1.12.42137 > 192.168.3.1.domain: 8183+ PTR? 99.200.250.142.in-addr.arpa. (45)
07:14:09.588545 IP 192.168.3.1.domain > 10.0.1.12.42137: 8183 1/0/0 PTR mad41s13-in-f3.1e100.net. (83)
07:14:09.747726 IP 10.0.1.12.57488 > mad41s13-in-f3.1e100.net.http: Flags [.], ack 20398, win 31590, length 0
07:14:09.748056 IP mad41s13-in-f3.1e100.net.http > 10.0.1.12.57488: Flags [.], ack 1, win 32349, length 0
07:14:11.796487 IP 10.0.1.12.37676 > 192.229.221.95.http: Flags [.], ack 18506, win 31691, length 0
07:14:11.796566 IP 10.0.1.12.37686 > 192.229.221.95.http: Flags [.], ack 18818, win 31691, length 0
07:14:11.796774 IP 192.229.221.95.http > 10.0.1.12.37676: Flags [.], ack 1, win 32352, length 0
07:14:11.796775 IP 192.229.221.95.http > 10.0.1.12.37686: Flags [.], ack 1, win 32352, length 0
07:14:11.799901 IP 10.0.1.12.45548 > a23-200-86-251.deploy.static.akamaitechnologies.com.http: Flags [.], ack 602785, win 65535, length 0
07:14:11.800118 IP a23-200-86-251.deploy.static.akamaitechnologies.com.http > 10.0.1.12.45548: Flags [.], ack 1, win 32471, length 0
07:14:11.808542 IP 10.0.1.12.43527 > 192.168.3.1.domain: 29430+ PTR? 95.221.229.192.in-addr.arpa. (45)
07:14:11.825803 IP 192.168.3.1.domain > 10.0.1.12.43527: 29430 NXDomain 0/1/0 (116)
07:14:11.826251 IP 10.0.1.12.44833 > 192.168.3.1.domain: 46871+ PTR? 251.86.200.23.in-addr.arpa. (44)
07:14:11.893510 IP 192.168.3.1.domain > 10.0.1.12.44833: 46871 1/0/0 PTR a23-200-86-251.deploy.static.akamaitechnologies.com. (109)
07:14:16.366952 IP 10.0.1.12.44742 > 192.168.3.1.domain: 56253+ A? example.com. (29)
07:14:16.369973 IP 192.168.3.1.domain > 10.0.1.12.44742: 56253 1/0/0 A 93.184.216.34 (45)
07:14:16.370550 IP 10.0.1.12.58940 > 93.184.216.34.http: Flags [S], seq 3694462500, win 32120, options [mss 1460,sackOK,TS val 3049036386 ecr 0,nop,wscale 7], length 0
07:14:16.464298 IP 93.184.216.34.http > 10.0.1.12.58940: Flags [S.], seq 20221, ack 3694462501, win 32768, options [mss 1460], length 0
07:14:16.464366 IP 10.0.1.12.58940 > 93.184.216.34.http: Flags [.], ack 1, win 32120, length 0
07:14:16.464733 IP 10.0.1.12.58940 > 93.184.216.34.http: Flags [P.], seq 1:420, ack 1, win 32120, length 419: HTTP: GET / HTTP/1.1
07:14:16.565020 IP 93.184.216.34.http > 10.0.1.12.58940: Flags [P.], seq 1:283, ack 420, win 32349, length 282: HTTP: HTTP/1.1 304 Not Modified
07:14:16.565101 IP 10.0.1.12.58940 > 93.184.216.34.http: Flags [.], ack 283, win 31838, length 0
07:14:19.732739 IP 10.0.1.12.57484 > mad41s13-in-f3.1e100.net.http: Flags [.], ack 1, win 31590, length 0
07:14:19.732962 IP mad41s13-in-f3.1e100.net.http > 10.0.1.12.57484: Flags [.], ack 1, win 32349, length 0
07:14:19.988059 IP 10.0.1.12.57488 > mad41s13-in-f3.1e100.net.http: Flags [.], ack 1, win 31590, length 0
07:14:19.988324 IP mad41s13-in-f3.1e100.net.http > 10.0.1.12.57488: Flags [.], ack 1, win 32349, length 0

Tshark:


kali@kali: ~
File Actions Edit View Help
kali@kali: ~ ×
kali@kali: ~ ×
(kali㉿kali)-[~]
$ tshark
Capturing on 'eth0'
1 0.000000000 10.0.1.12 → 34.149.100.209 TLSv1.2 100 Application Data
2 0.000505679 10.0.1.12 → 34.149.100.209 TLSv1.2 85 Encrypted Alert
3 0.000688366 34.149.100.209 → 10.0.1.12 TCP 60 443 → 51494 [ACK] Seq=1 Ack=78 Win=32599 Len=0
4 0.000963732 10.0.1.12 → 34.149.100.209 TCP 54 51494 → 443 [FIN, ACK] Seq=78 Ack=1 Win=65535 Len=0
5 0.001262851 34.149.100.209 → 10.0.1.12 TCP 60 443 → 51494 [ACK] Seq=1 Ack=79 Win=32598 Len=0
6 0.009469760 34.149.100.209 → 10.0.1.12 TCP 60 443 → 51494 [FIN, ACK] Seq=1 Ack=79 Win=32598 Len=0
7 0.009495496 10.0.1.12 → 34.149.100.209 TCP 54 51494 → 443 [ACK] Seq=79 Ack=2 Win=64732 Len=0


kali@kali: ~
File Actions Edit View Help
kali@kali: ~ ×
kali@kali: ~ ×
(kali㉿kali)-[~]
$ tshark
Capturing on 'eth0'
1 0.000000000 10.0.1.12 → 93.184.216.34 HTTP 473 GET / HTTP/1.1
2 0.098317966 93.184.216.34 → 10.0.1.12 HTTP 336 HTTP/1.1 304 Not Modified
3 0.098376999 10.0.1.12 → 93.184.216.34 TCP 54 58940 → 80 [ACK] Seq=420 Ack=283 Win=31624 Len=0
4 9.002215948 10.0.1.12 → 35.244.181.201 TLSv1.2 100 Application Data
5 9.011908773 35.244.181.201 → 10.0.1.12 TLSv1.2 100 Application Data
6 9.055314670 10.0.1.12 → 35.244.181.201 TCP 54 44480 → 443 [ACK] Seq=47 Ack=47 Win=30660 Len=0
Example Domain


kali@kali: ~
File Actions Edit View Help
kali@kali: ~ ×
kali@kali: ~ ×
(kali㉿kali)-[~]
$ tshark
Capturing on 'eth0'
1 0.000000000 10.0.1.12 → 93.184.216.34 HTTP 473 GET / HTTP/1.1
2 0.098317966 93.184.216.34 → 10.0.1.12 HTTP 336 HTTP/1.1 304 Not Modified
3 0.098376999 10.0.1.12 → 93.184.216.34 TCP 54 58940 → 80 [ACK] Seq=420 Ack=283 Win=31624 Len=0
4 9.002215948 10.0.1.12 → 35.244.181.201 TLSv1.2 100 Application Data
5 9.011908773 35.244.181.201 → 10.0.1.12 TLSv1.2 100 Application Data
6 9.055314670 10.0.1.12 → 35.244.181.201 TCP 54 44480 → 443 [ACK] Seq=47 Ack=47 Win=30660 Len=0
7 10.142596266 10.0.1.12 → 93.184.216.34 TCP 54 [TCP Keep-Alive] 58940 → 80 [ACK] Seq=419 Ack=283 Win=31624 Len=0
8 10.142847949 93.184.216.34 → 10.0.1.12 TCP 60 [TCP Keep-Alive ACK] 80 → 58940 [ACK] Seq=283 Ack=420 Win=31511 Len=0
9 20.033803279 10.0.1.13 → 10.0.1.12 ICMP 98 Echo (ping) request id=0×0002, seq=1/256, ttl=64
10 20.033843566 10.0.1.12 → 10.0.1.13 ICMP 98 Echo (ping) reply id=0×0002, seq=1/256, ttl=64 (request in 9)
11 20.382620100 10.0.1.12 → 93.184.216.34 TCP 54 [TCP Keep-Alive] 58940 → 80 [ACK] Seq=419 Ack=283 Win=31624 Len=0
12 20.382897679 93.184.216.34 → 10.0.1.12 TCP 60 [TCP Keep-Alive ACK] 80 → 58940 [ACK] Seq=283 Ack=420 Win=31511 Len=0
13 21.050091347 10.0.1.13 → 10.0.1.12 ICMP 98 Echo (ping) request id=0×0002, seq=2/512, ttl=64
14 21.050116893 10.0.1.12 → 10.0.1.13 ICMP 98 Echo (ping) reply id=0×0002, seq=2/512, ttl=64 (request in 13)
15 22.073151031 10.0.1.13 → 10.0.1.12 ICMP 98 Echo (ping) request id=0×0002, seq=3/768, ttl=64
16 22.073178359 10.0.1.12 → 10.0.1.13 ICMP 98 Echo (ping) reply id=0×0002, seq=3/768, ttl=64 (request in 15)
17 23.096369217 10.0.1.13 → 10.0.1.12 ICMP 98 Echo (ping) request id=0×0002, seq=4/1024, ttl=64
18 23.096405607 10.0.1.12 → 10.0.1.13 ICMP 98 Echo (ping) reply id=0×0002, seq=4/1024, ttl=64 (request in 17)
19 25.175671241 PCSSystemtec_2b:c0:9a → PCSSystemtec_f6:db:d7 ARP 60 Who has 10.0.1.12? Tell 10.0.1.13
20 25.175693242 PCSSystemtec_f6:db:d7 → PCSSystemtec_2b:c0:9a ARP 42 10.0.1.12 is at 08:00:27:f6:db:d7
21 25.246613873 PCSSystemtec_f6:db:d7 → PCSSystemtec_2b:c0:9a ARP 42 Who has 10.0.1.13? Tell 10.0.1.12
22 25.247459629 PCSSystemtec_2b:c0:9a → PCSSystemtec_f6:db:d7 ARP 60 10.0.1.13 is at 08:00:27:2b:c0:9a
23 30.622626477 10.0.1.12 → 93.184.216.34 TCP 54 [TCP Keep-Alive] 58940 → 80 [ACK] Seq=419 Ack=283 Win=31624 Len=0
24 30.622964111 93.184.216.34 → 10.0.1.12 TCP 60 [TCP Keep-Alive ACK] 80 → 58940 [ACK] Seq=283 Ack=420 Win=31511 Len=0


kali@kali: ~
File Actions Edit View Help
kali@kali: ~ ×
kali@kali: ~ ×
5 9.011908773 35.244.181.201 → 10.0.1.12 TLSv1.2 100 Application Data
6 9.055314670 10.0.1.12 → 35.244.181.201 TCP 54 44480 → 443 [ACK] Seq=47 Ack=47 Win=30660 Len=0
7 10.142596266 10.0.1.12 → 93.184.216.34 TCP 54 [TCP Keep-Alive] 58940 → 80 [ACK] Seq=419 Ack=283 Win=31624 Len=0
8 10.142847949 93.184.216.34 → 10.0.1.12 TCP 60 [TCP Keep-Alive ACK] 80 → 58940 [ACK] Seq=283 Ack=420 Win=31511 Len=0
9 20.033803279 10.0.1.13 → 10.0.1.12 ICMP 98 Echo (ping) request id=0×0002, seq=1/256, ttl=64
10 20.033843566 10.0.1.12 → 10.0.1.13 ICMP 98 Echo (ping) reply id=0×0002, seq=1/256, ttl=64 (request in 9)
11 20.382620100 10.0.1.12 → 93.184.216.34 TCP 54 [TCP Keep-Alive] 58940 → 80 [ACK] Seq=419 Ack=283 Win=31624 Len=0
12 20.382897679 93.184.216.34 → 10.0.1.12 TCP 60 [TCP Keep-Alive ACK] 80 → 58940 [ACK] Seq=283 Ack=420 Win=31511 Len=0
13 21.050091347 10.0.1.13 → 10.0.1.12 ICMP 98 Echo (ping) request id=0×0002, seq=2/512, ttl=64
14 21.050116893 10.0.1.12 → 10.0.1.13 ICMP 98 Echo (ping) reply id=0×0002, seq=2/512, ttl=64 (request in 13)
15 22.073151031 10.0.1.13 → 10.0.1.12 ICMP 98 Echo (ping) request id=0×0002, seq=3/768, ttl=64
16 22.073178359 10.0.1.12 → 10.0.1.13 ICMP 98 Echo (ping) reply id=0×0002, seq=3/768, ttl=64 (request in 15)
17 23.096369217 10.0.1.13 → 10.0.1.12 ICMP 98 Echo (ping) request id=0×0002, seq=4/1024, ttl=64
18 23.096405607 10.0.1.12 → 10.0.1.13 ICMP 98 Echo (ping) reply id=0×0002, seq=4/1024, ttl=64 (request in 17)
19 25.175671241 PCSSystemtec_2b:c0:9a → PCSSystemtec_f6:db:d7 ARP 60 Who has 10.0.1.12? Tell 10.0.1.13
20 25.175693242 PCSSystemtec_f6:db:d7 → PCSSystemtec_2b:c0:9a ARP 42 10.0.1.12 is at 08:00:27:f6:db:d7
21 25.246613873 PCSSystemtec_f6:db:d7 → PCSSystemtec_2b:c0:9a ARP 42 Who has 10.0.1.13? Tell 10.0.1.12
22 25.247459629 PCSSystemtec_2b:c0:9a → PCSSystemtec_f6:db:d7 ARP 60 10.0.1.13 is at 08:00:27:2b:c0:9a
23 30.622626477 10.0.1.12 → 93.184.216.34 TCP 54 [TCP Keep-Alive] 58940 → 80 [ACK] Seq=419 Ack=283 Win=31624 Len=0
24 30.622964111 93.184.216.34 → 10.0.1.12 TCP 60 [TCP Keep-Alive ACK] 80 → 58940 [ACK] Seq=283 Ack=420 Win=31511 Len=0
25 40.862761787 10.0.1.12 → 93.184.216.34 TCP 54 [TCP Keep-Alive] 58940 → 80 [ACK] Seq=419 Ack=283 Win=31624 Len=0
26 40.862997718 93.184.216.34 → 10.0.1.12 TCP 60 [TCP Keep-Alive ACK] 80 → 58940 [ACK] Seq=283 Ack=420 Win=31511 Len=0
27 45.982954842 PCSSystemtec_f6:db:d7 → 52:54:00:12:35:00 ARP 42 Who has 10.0.1.1? Tell 10.0.1.12
28 45.983424631 52:54:00:12:35:00 → PCSSystemtec_f6:db:d7 ARP 60 10.0.1.1 is at 52:54:00:12:35:00
29 46.195792846 PCSSystemtec_d4:54:10 → Broadcast ARP 60 Who has 10.0.1.12? Tell 10.0.1.14
30 46.195862443 PCSSystemtec_f6:db:d7 → PCSSystemtec_d4:54:10 ARP 42 10.0.1.12 is at 08:00:27:f6:db:d7
31 46.196248345 10.0.1.14 → 10.0.1.12 ICMP 98 Echo (ping) request id=0×0002, seq=1/256, ttl=64
32 46.196312745 10.0.1.12 → 10.0.1.14 ICMP 98 Echo (ping) reply id=0×0002, seq=1/256, ttl=64 (request in 31)
33 47.196771260 10.0.1.14 → 10.0.1.12 ICMP 98 Echo (ping) request id=0×0002, seq=2/512, ttl=64
34 47.196809804 10.0.1.12 → 10.0.1.14 ICMP 98 Echo (ping) reply id=0×0002, seq=2/512, ttl=64 (request in 33)
35 48.209735774 10.0.1.14 → 10.0.1.12 ICMP 98 Echo (ping) request id=0×0002, seq=3/768, ttl=64
36 48.209759427 10.0.1.12 → 10.0.1.14 ICMP 98 Echo (ping) reply id=0×0002, seq=3/768, ttl=64 (request in 35)
37 49.233254820 10.0.1.14 → 10.0.1.12 ICMP 98 Echo (ping) request id=0×0002, seq=4/1024, ttl=64
38 49.233284191 10.0.1.12 → 10.0.1.14 ICMP 98 Echo (ping) reply id=0×0002, seq=4/1024, ttl=64 (request in 37)
39 50.256856116 10.0.1.14 → 10.0.1.12 ICMP 98 Echo (ping) request id=0×0002, seq=5/1280, ttl=64
40 50.256881331 10.0.1.12 → 10.0.1.14 ICMP 98 Echo (ping) reply id=0×0002, seq=5/1280, ttl=64 (request in 39)
41 51.103936369 10.0.1.12 → 93.184.216.34 TCP 54 [TCP Keep-Alive] 58940 → 80 [ACK] Seq=419 Ack=283 Win=31624 Len=0
42 51.104196394 93.184.216.34 → 10.0.1.12 TCP 60 [TCP Keep-Alive ACK] 80 → 58940 [ACK] Seq=283 Ack=420 Win=31511 Len=0
43 51.256709710 10.0.1.14 → 10.0.1.12 ICMP 98 Echo (ping) request id=0×0002, seq=6/1536, ttl=64
44 51.256737549 10.0.1.12 → 10.0.1.14 ICMP 98 Echo (ping) reply id=0×0002, seq=6/1536, ttl=64 (request in 43)
45 51.428681578 PCSSystemtec_f6:db:d7 → PCSSystemtec_d4:54:10 ARP 42 Who has 10.0.1.14? Tell 10.0.1.12
46 51.429192965 PCSSystemtec_d4:54:10 → PCSSystemtec_f6:db:d7 ARP 60 10.0.1.14 is at 08:00:27:d4:54:10