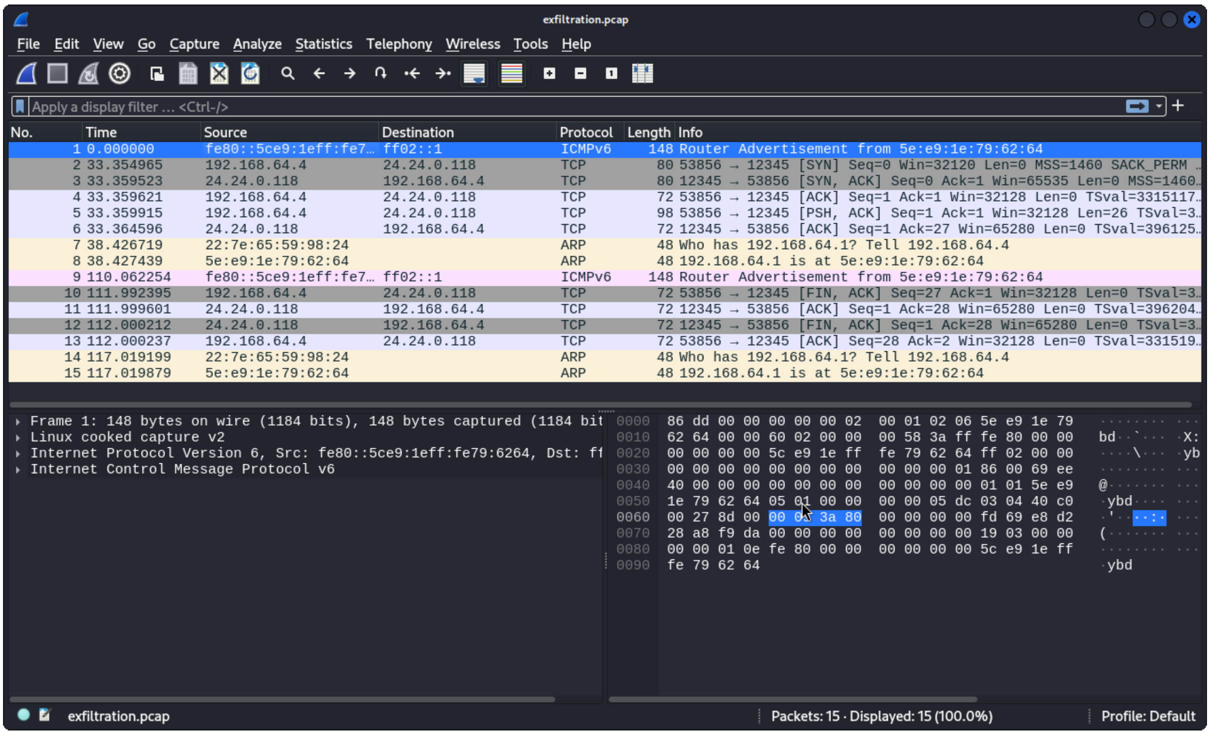
Phase 3: Reconstructing the Data Exfiltration

Plot Point: The investigator uses network forensics to trace how the stolen data was exfiltrated from the company’s network to an external destination.

The investigator opened the PCAP file in Wireshark, applying a filter for HTTPS traffic. A stream of packets stood out—large outbound transfers to an IP address not on the company’s whitelist. Reconstructing the stream, they found encrypted data being uploaded to competitorcorp.sharepoint.com. Cross-referencing the DNS query logs, they confirmed the domain was resolved during the breach. “He sent it straight to the competitor,” the investigator said, shaking their head. NetFlow data sealed the case—a massive spike in outbound traffic at 2:15 AM, matching the database queries to the second.

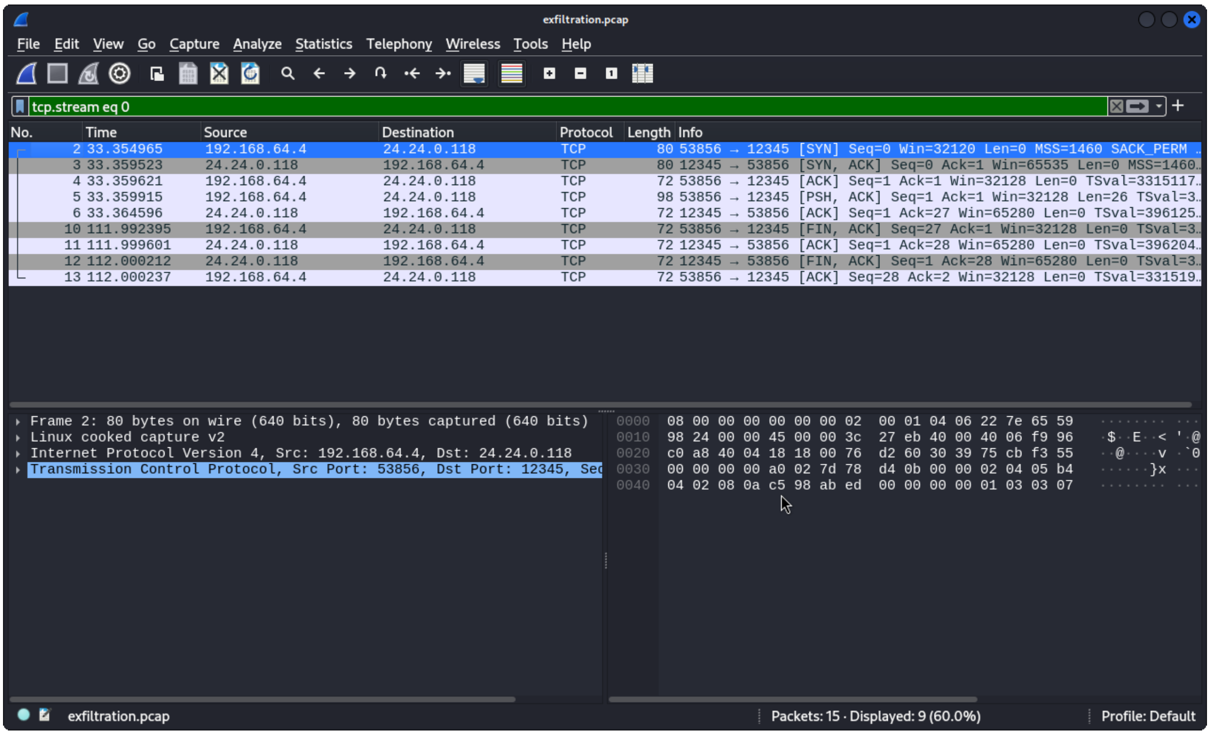

exfiltration.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time        Source                    Destination    Protocol Length Info
    1 0.000000    fe80::5ce9:1eff:fe7…      ff02::1        ICMPv6    148 Router Advertisement from 5e:e9:1e:79:62:64
    2 33.354965   192.168.64.4              24.24.0.118    TCP        80 53856 → 12345 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM …
    3 33.359523   24.24.0.118               192.168.64.4   TCP        80 12345 → 53856 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460…
    4 33.359621   192.168.64.4              24.24.0.118    TCP        72 53856 → 12345 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3315117…
    5 33.359915   192.168.64.4              24.24.0.118    TCP        98 53856 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=32128 Len=26 TSval=3…
    6 33.364596   24.24.0.118               192.168.64.4   TCP        72 12345 → 53856 [ACK] Seq=1 Ack=27 Win=65280 Len=0 TSval=396125…
    7 38.426719   22:7e:65:59:98:24                        ARP        48 Who has 192.168.64.1? Tell 192.168.64.4
    8 38.427439   5e:e9:1e:79:62:64                        ARP        48 192.168.64.1 is at 5e:e9:1e:79:62:64
    9 110.062254  fe80::5ce9:1eff:fe7…      ff02::1        ICMPv6    148 Router Advertisement from 5e:e9:1e:79:62:64
   10 111.992395  192.168.64.4              24.24.0.118    TCP        72 53856 → 12345 [FIN, ACK] Seq=27 Ack=1 Win=32128 Len=0 TSval=3…
   11 111.999601  24.24.0.118               192.168.64.4   TCP        72 12345 → 53856 [ACK] Seq=1 Ack=28 Win=65280 Len=0 TSval=396204…
   12 112.000212  24.24.0.118               192.168.64.4   TCP        72 12345 → 53856 [FIN, ACK] Seq=1 Ack=28 Win=65280 Len=0 TSval=3…
   13 112.000237  192.168.64.4              24.24.0.118    TCP        72 53856 → 12345 [ACK] Seq=28 Ack=2 Win=32128 Len=0 TSval=331519…
   14 117.019199  22:7e:65:59:98:24                        ARP        48 Who has 192.168.64.1? Tell 192.168.64.4
   15 117.019879  5e:e9:1e:79:62:64                        ARP        48 192.168.64.1 is at 5e:e9:1e:79:62:64
```

```
› Frame 1: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bit
› Linux cooked capture v2
› Internet Protocol Version 6, Src: fe80::5ce9:1eff:fe79:6264, Dst: ff
› Internet Control Message Protocol v6
```

```
0000  86 dd 00 00 00 00 00 02  00 01 02 06 5e e9 1e 79   ········ ···
0010  62 64 00 00 60 02 00 00  00 58 3a ff fe 80 00 00   bd··`··· ·X:
0020  00 00 00 00 5c e9 1e ff  fe 79 62 64 ff 02 00 00   ····\··· ·yb
0030  00 00 00 00 00 00 00 00  00 00 00 01 86 00 69 ee   ········ ···
0040  40 00 00 00 00 00 00 00  00 00 00 00 01 01 5e e9   @······· ···
0050  1e 79 62 64 05 01 00 00  00 00 05 dc 03 04 40 c0   ·ybd···· ···
0060  00 27 8d 00 00 00 3a 80  00 00 00 00 fd 69 e8 d2   ·'····:· ···
0070  28 a8 f9 da 00 00 00 00  00 00 00 00 19 03 00 00   (······· ···
0080  00 00 01 0e fe 80 00 00  00 00 00 00 5c e9 1e ff   ········ ···
0090  fe 79 62 64                                        ·ybd
```

exfiltration.pcap | Packets: 15 · Displayed: 15 (100.0%) | Profile: Default



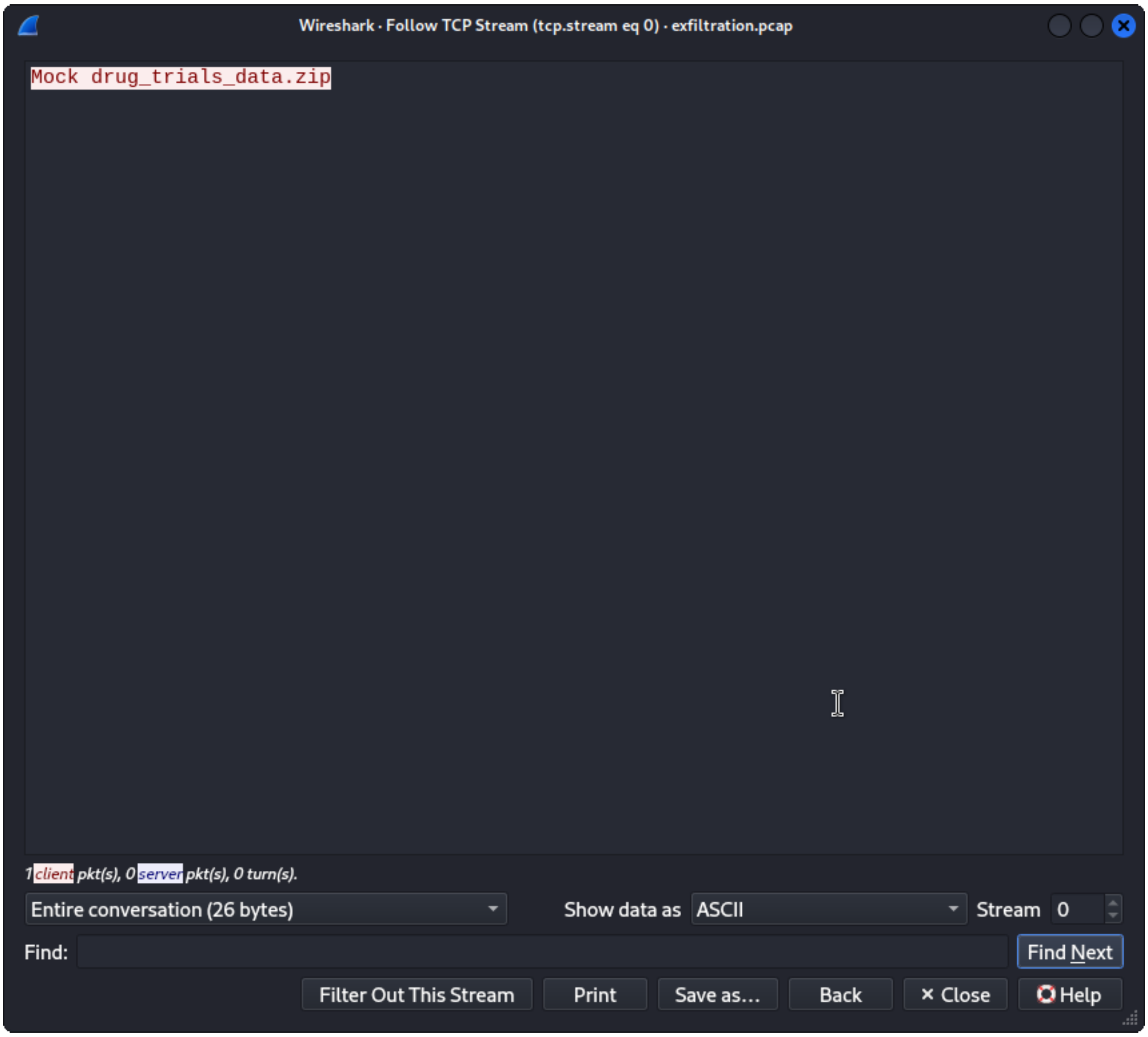
exfiltration.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.stream eq 0
```

```
No.  Time        Source          Destination     Protocol Length Info
   2 33.354965   192.168.64.4    24.24.0.118     TCP      80 53856 → 12345 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM …
   3 33.359523   24.24.0.118     192.168.64.4    TCP      80 12345 → 53856 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460…
   4 33.359621   192.168.64.4    24.24.0.118     TCP      72 53856 → 12345 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3315117…
   5 33.359915   192.168.64.4    24.24.0.118     TCP      98 53856 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=32128 Len=26 TSval=3…
   6 33.364596   24.24.0.118     192.168.64.4    TCP      72 12345 → 53856 [ACK] Seq=1 Ack=27 Win=65280 Len=0 TSval=396125…
  10 111.992395  192.168.64.4    24.24.0.118     TCP      72 53856 → 12345 [FIN, ACK] Seq=27 Ack=1 Win=32128 Len=0 TSval=3…
  11 111.999601  24.24.0.118     192.168.64.4    TCP      72 12345 → 53856 [ACK] Seq=1 Ack=28 Win=65280 Len=0 TSval=396204…
  12 112.000212  24.24.0.118     192.168.64.4    TCP      72 12345 → 53856 [FIN, ACK] Seq=1 Ack=28 Win=65280 Len=0 TSval=3…
  13 112.000237  192.168.64.4    24.24.0.118     TCP      72 53856 → 12345 [ACK] Seq=28 Ack=2 Win=32128 Len=0 TSval=331519…
```

```
› Frame 2: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
› Linux cooked capture v2
› Internet Protocol Version 4, Src: 192.168.64.4, Dst: 24.24.0.118
› Transmission Control Protocol, Src Port: 53856, Dst Port: 12345, Seq
```

```
0000  08 00 00 00 00 00 00 02  00 01 04 06 22 7e 65 59   ········ ···
0010  98 24 00 00 45 00 00 3c  27 eb 40 00 40 06 f9 96   ·$··E··< '·@
0020  c0 a8 40 04 18 18 00 76  d2 60 30 39 75 cb f3 55   ··@····v ·`0
0030  00 00 00 00 a0 02 7d 78  d4 0b 00 00 02 04 05 b4   ······}x ···
0040  04 02 08 0a c5 98 ab ed  00 00 00 00 01 03 03 07   ········ ···
```



Wireshark · Follow TCP Stream (tcp.stream eq 0) · exfiltration.pcap

```
Mock drug_trials_data.zip
```

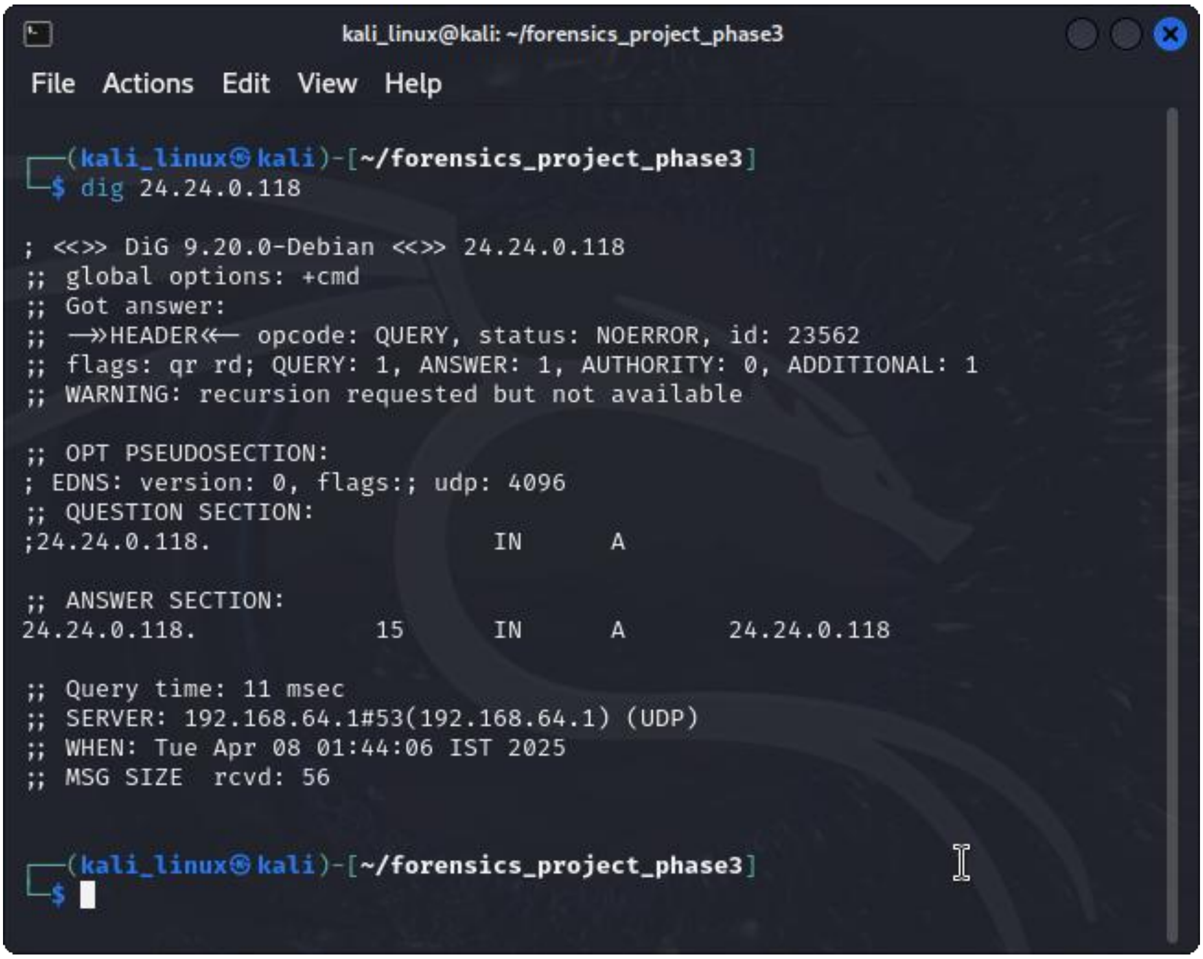
1 client pkt(s), 0 server pkt(s), 0 turn(s).

Entire conversation (26 bytes)

Show data as ASCII

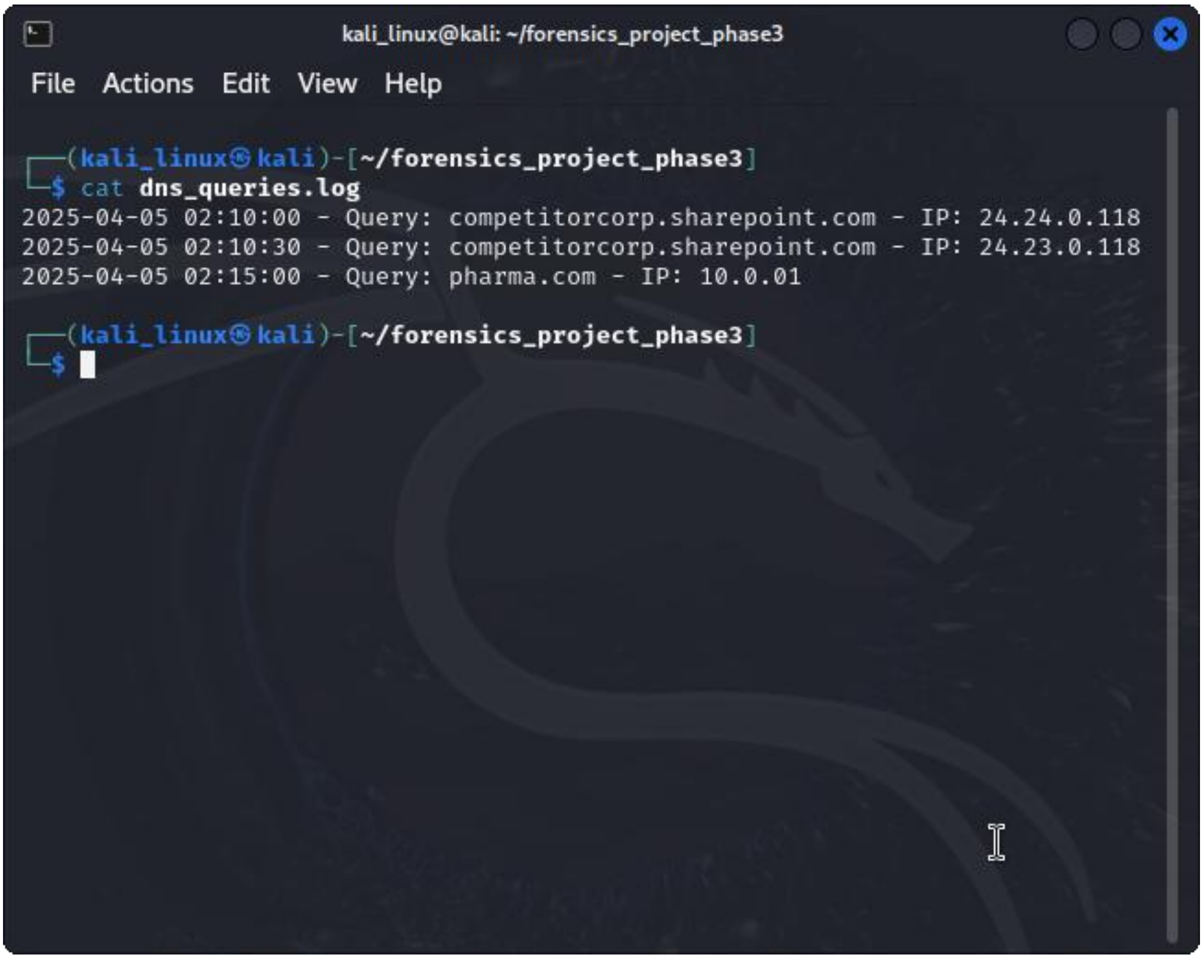
Stream 0

Find:
Find Next
Filter Out This Stream
Print
Save as…
Back
× Close
Help

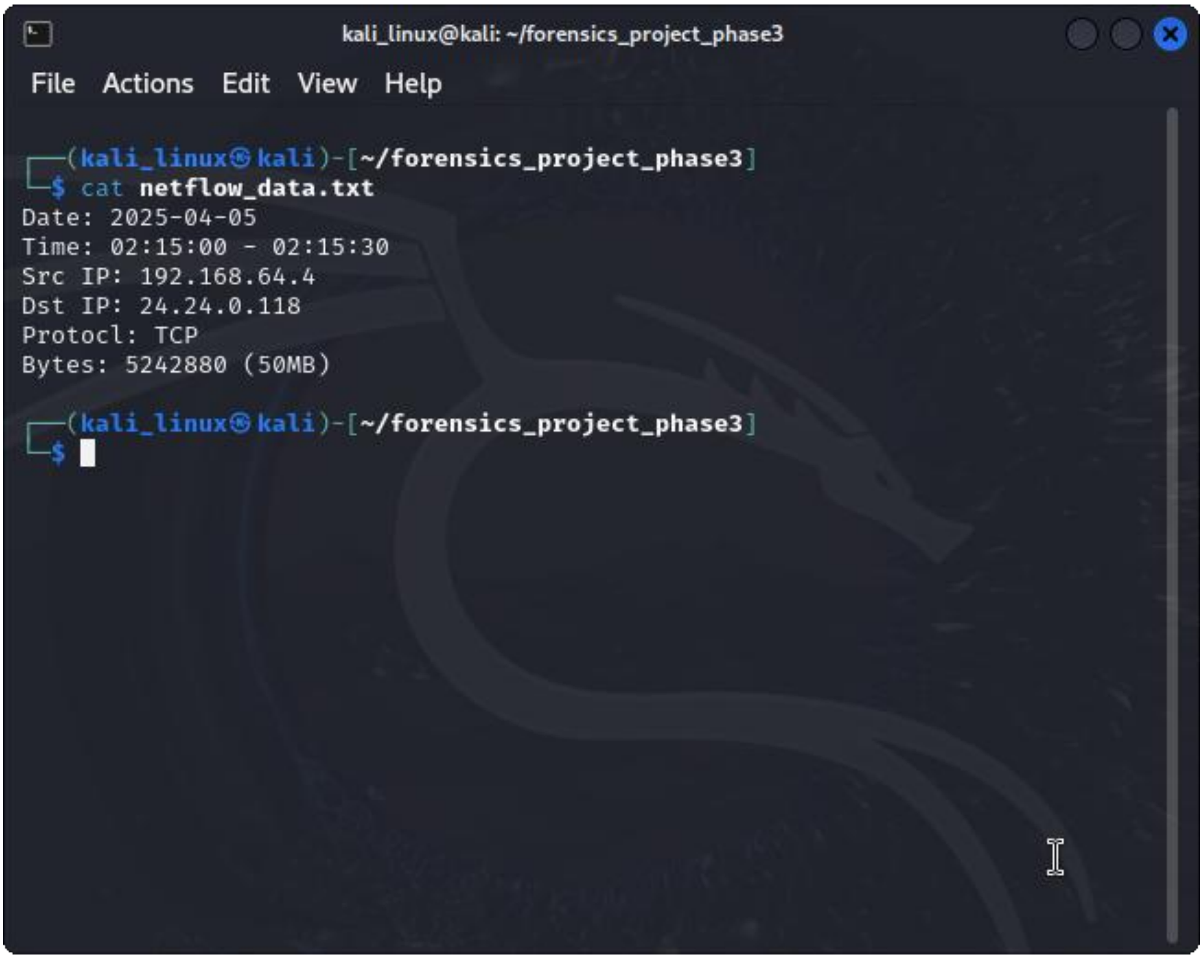


kali_linux@kali: ~/forensics_project_phase3
File Actions Edit View Help

```
┌──(kali_linux㉿kali)-[~/forensics_project_phase3]
└─$ dig 24.24.0.118

; <<>> DiG 9.20.0-Debian <<>> 24.24.0.118
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23562
;; flags: qr rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;24.24.0.118.                   IN      A

;; ANSWER SECTION:
24.24.0.118.            15      IN      A       24.24.0.118

;; Query time: 11 msec
;; SERVER: 192.168.64.1#53(192.168.64.1) (UDP)
;; WHEN: Tue Apr 08 01:44:06 IST 2025
;; MSG SIZE  rcvd: 56


┌──(kali_linux㉿kali)-[~/forensics_project_phase3]
└─$ 
```

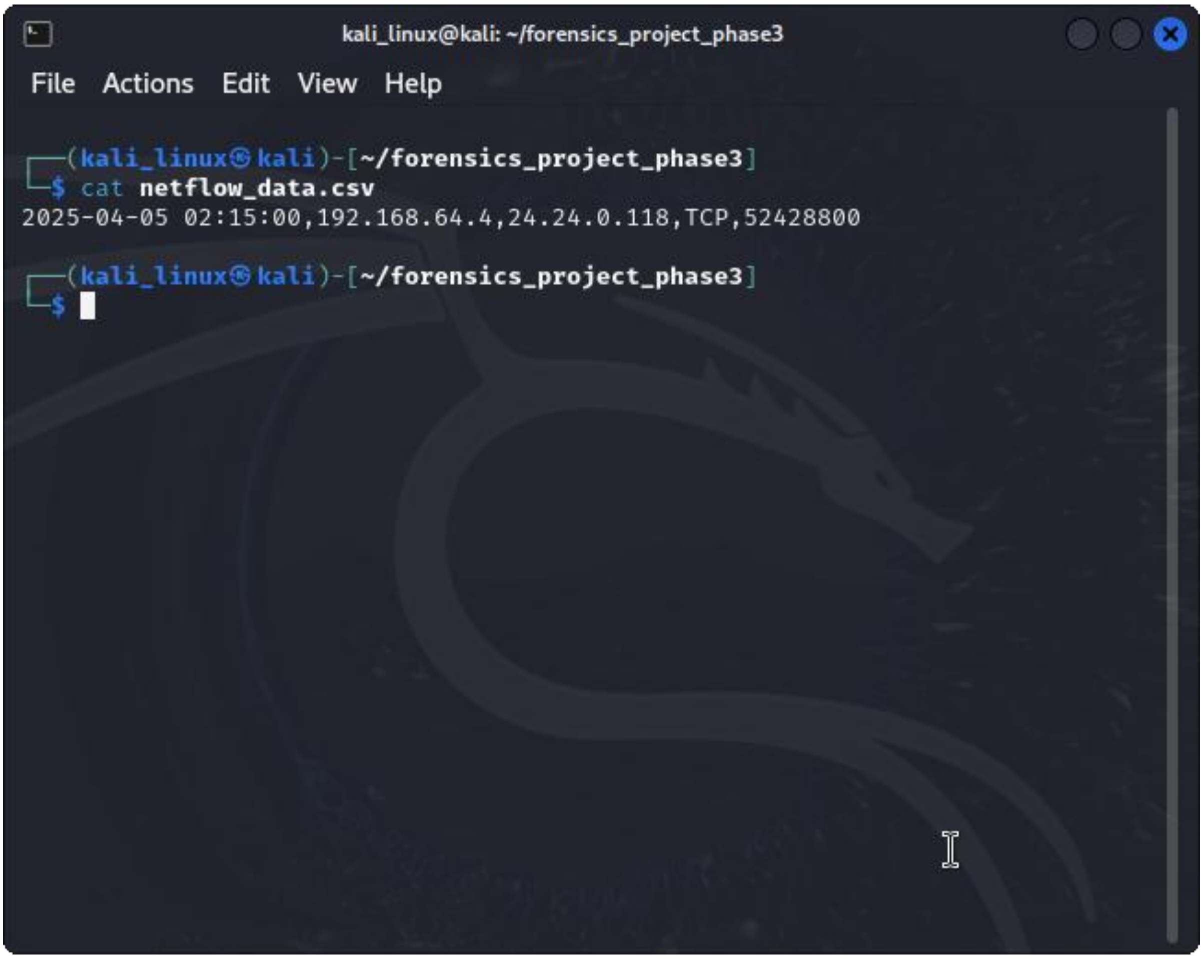

kali_linux@kali: ~/forensics_project_phase3
File Actions Edit View Help

```
┌──(kali_linux㉿kali)-[~/forensics_project_phase3]
└─$ cat dns_queries.log
2025-04-05 02:10:00 - Query: competitorcorp.sharepoint.com - IP: 24.24.0.118
2025-04-05 02:10:30 - Query: competitorcorp.sharepoint.com - IP: 24.23.0.118
2025-04-05 02:15:00 - Query: pharma.com - IP: 10.0.01

┌──(kali_linux㉿kali)-[~/forensics_project_phase3]
└─$ 
```



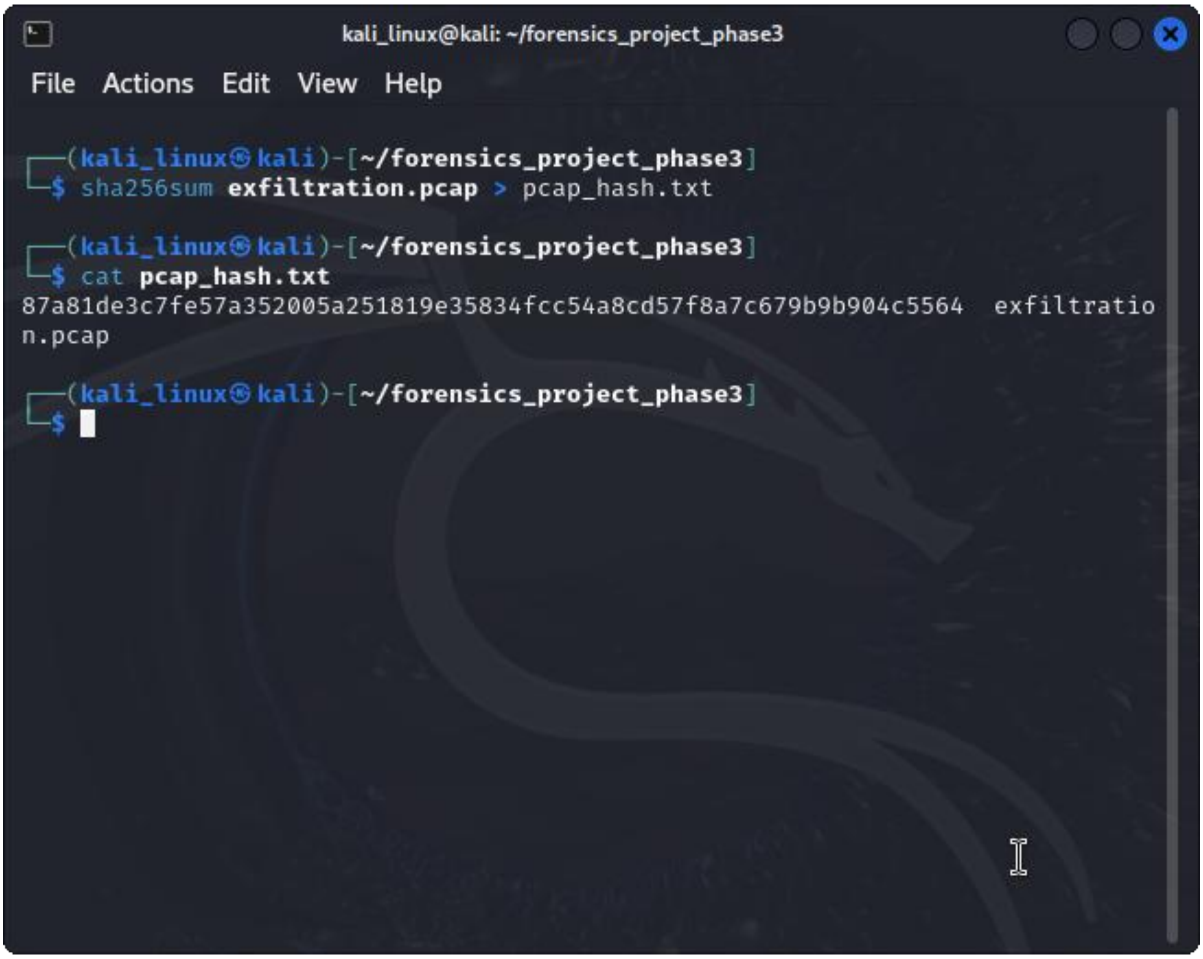
kali_linux@kali: ~/forensics_project_phase3
File Actions Edit View Help

```
┌──(kali_linux㉿kali)-[~/forensics_project_phase3]
└─$ cat netflow_data.txt
Date: 2025-04-05
Time: 02:15:00 - 02:15:30
Src IP: 192.168.64.4
Dst IP: 24.24.0.118
Protocl: TCP
Bytes: 5242880 (50MB)

┌──(kali_linux㉿kali)-[~/forensics_project_phase3]
└─$ 
```

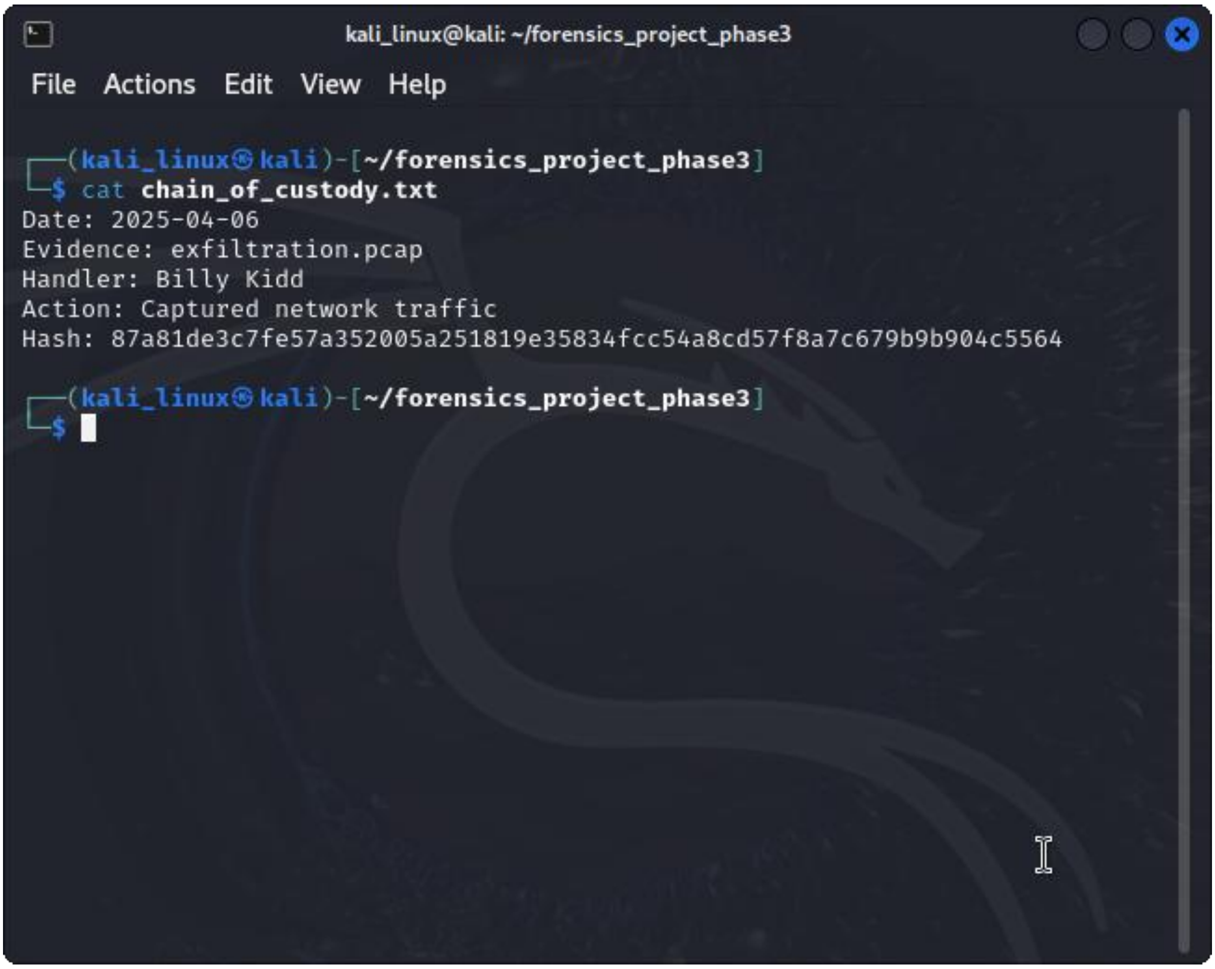


kali_linux@kali: ~/forensics_project_phase3
File Actions Edit View Help

```
┌──(kali_linux㉿kali)-[~/forensics_project_phase3]
└─$ cat netflow_data.csv
2025-04-05 02:15:00,192.168.64.4,24.24.0.118,TCP,52428800

┌──(kali_linux㉿kali)-[~/forensics_project_phase3]
└─$ 
```



```
┌──(kali_linux㉿kali)-[~/forensics_project_phase3]
└─$ sha256sum exfiltration.pcap > pcap_hash.txt

┌──(kali_linux㉿kali)-[~/forensics_project_phase3]
└─$ cat pcap_hash.txt
87a81de3c7fe57a352005a251819e35834fcc54a8cd57f8a7c679b9b904c5564  exfiltratio
n.pcap

┌──(kali_linux㉿kali)-[~/forensics_project_phase3]
└─$ 
```



kali_linux@kali: ~/forensics_project_phase3
File Actions Edit View Help

```
┌──(kali_linux㉿kali)-[~/forensics_project_phase3]
└─$ cat chain_of_custody.txt
Date: 2025-04-06
Evidence: exfiltration.pcap
Handler: Billy Kidd
Action: Captured network traffic
Hash: 87a81de3c7fe57a352005a251819e35834fcc54a8cd57f8a7c679b9b904c5564

┌──(kali_linux㉿kali)-[~/forensics_project_phase3]
└─$ 
```

Phase 4: Following the Data to the Cloud

Plot Point: The investigator traces the stolen data to a cloud storage service, confirming the exfiltration and identifying the recipient.

The investigator stared at the subpoenaed SharePoint logs, a digital breadcrumb trail leading to the stolen data. An upload event at 2:20 AM showed drug_trials_data.zip being transferred from an IP address geolocated to John Smith’s home address. The file’s MD5 hash matched the one recovered from his workstation—irrefutable proof. Digging into the API access logs, they found evidence of a scripted upload, confirming premeditation. “He thought he could hide behind the cloud,” the investigator said, “but the logs don’t lie.”