HTTPS-Decryption-And-Analysis-Wireshark

https://github.com/ahsanjunaid/HTTPS-Decryption-And-Analysis-Wireshark

Introduction

This documentation provides a detailed walkthrough of the steps I took to analyze malicious traffic in a HTTPS network using Wireshark. The objectives were:

- To decrypt HTTPS data secured with a TLS certificate
- Identify the type of malware
- Determine the infected system.

Setup

Wireshark:	Install the latest version of Wireshark on your system. You can download it from wireshark.org.
VirusTotal:	To analyze the malware DLL using VirusTotal.

Steps

1. Download and Extract Files

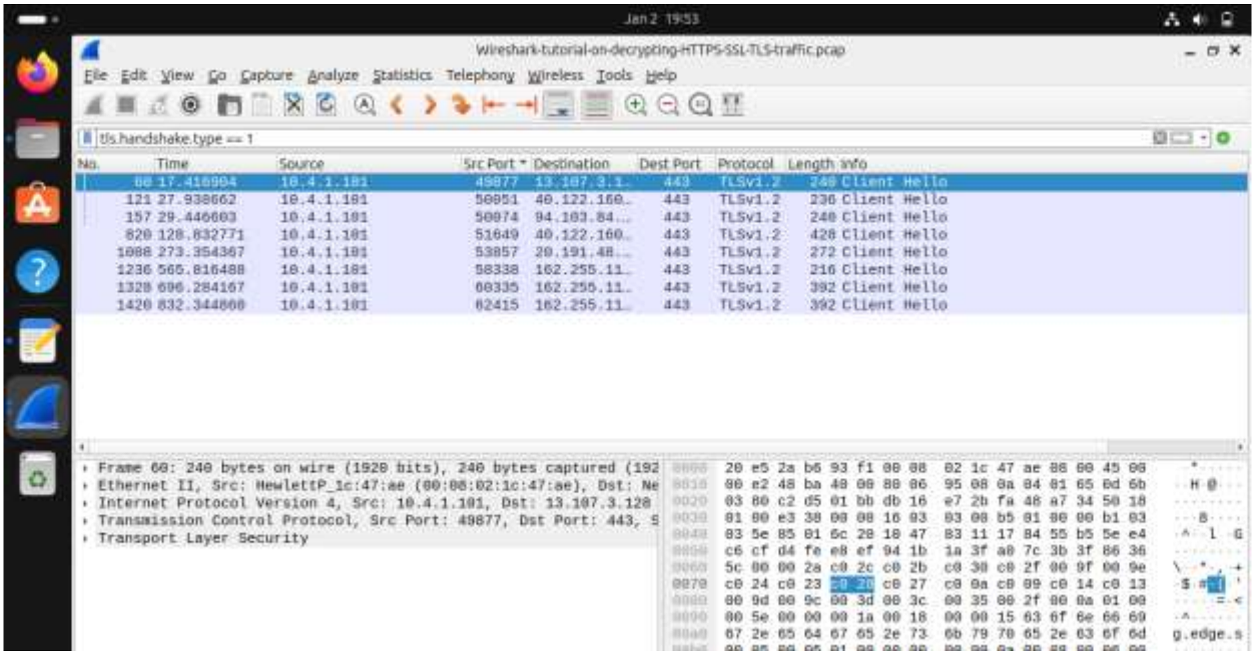
- Download the zip file, named "Materials" from the GitHub repository.
- Extract the files.

2. Open Pcap File with Wireshark

- Open Wireshark and use it to load the pcap file provided in the extracted files.
- It's important to note that sudo privileges are not required for this step since we are only analyzing, not capturing packets.

3. Filter TLS Handshake

- Apply a display filter to show successful TLS handshakes (`tls.handshake.type == 1`).
- Follow the TLS stream to view the encrypted data exchanged during the handshake.


Jan 2 19:53
Wireshark-tutorial-on-decrypting-HTTPS-SSL-TLS-traffic.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tls.handshake.type == 1
```

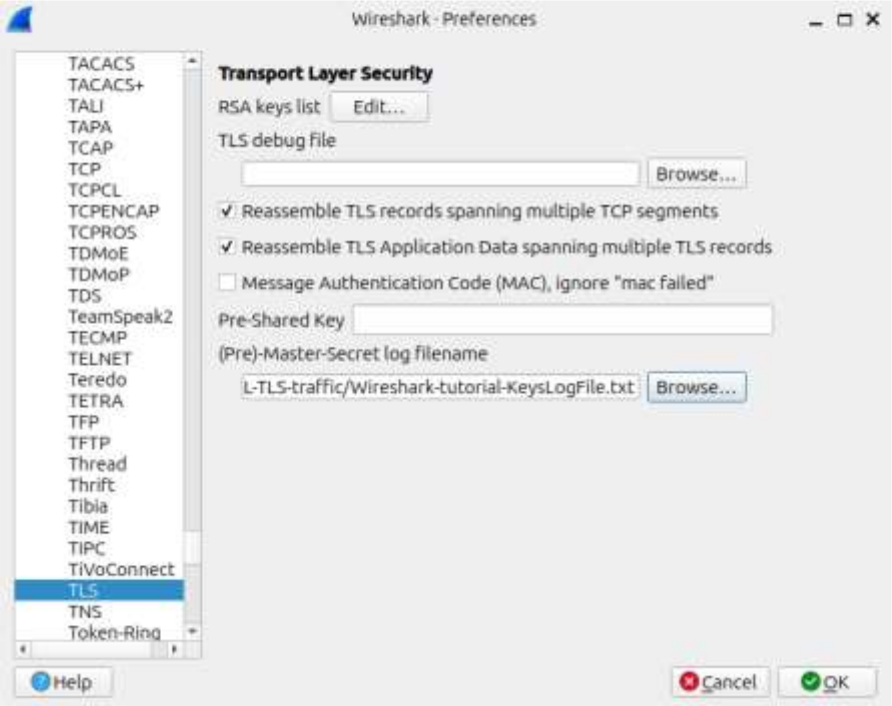
```
No.   Time         Source      Src Port  Destination   Dest Port  Protocol  Length Info
   60 17.416904    10.4.1.101  49877     13.107.3.1..  443        TLSv1.2   240 Client Hello
  121 27.938662    10.4.1.101  50051     40.122.160..  443        TLSv1.2   236 Client Hello
  157 29.446603    10.4.1.101  50074     94.103.84...  443        TLSv1.2   240 Client Hello
  820 128.832771   10.4.1.101  51649     40.122.160..  443        TLSv1.2   428 Client Hello
 1088 273.354367   10.4.1.101  53857     20.191.48...  443        TLSv1.2   272 Client Hello
 1236 565.816488   10.4.1.101  58338     162.255.11..  443        TLSv1.2   216 Client Hello
 1328 696.284167   10.4.1.101  60335     162.255.11..  443        TLSv1.2   392 Client Hello
 1420 832.344868   10.4.1.101  62415     162.255.11..  443        TLSv1.2   392 Client Hello
```

```
› Frame 60: 240 bytes on wire (1920 bits), 240 bytes captured (192
› Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Ne
› Internet Protocol Version 4, Src: 10.4.1.101, Dst: 13.107.3.128
› Transmission Control Protocol, Src Port: 49877, Dst Port: 443, S
› Transport Layer Security
```

```
0000  20 e5 2a b6 93 f1 00 08  02 1c 47 ae 08 00 45 00
0010  00 e2 48 ba 40 00 80 06  95 08 0a 04 01 65 0d 6b     H @
0020  03 80 c2 d5 01 bb db 16  e7 2b fa 48 a7 34 50 18
0030  01 00 e3 38 00 00 16 03  03 00 b5 01 00 00 b1 03      8
0040  03 5e 85 01 6c 20 18 47  83 11 17 84 55 b5 5e e4   ^  l  G
0050  c6 cf d4 fe e8 ef 94 1b  1a 3f a0 7c 3b 3f 86 36
0060  5c 00 00 2a c0 2c c0 2b  c0 30 c0 2f 00 9f 00 9e  \  * , +
0070  c0 24 c0 23 c0 28 c0 27  c0 0a c0 09 c0 14 c0 13   $ #( '
0080  00 9d 00 9c 00 3d 00 3c  00 35 00 2f 00 0a 01 00        = <
0090  00 5e 00 00 00 1a 00 18  00 00 15 63 6f 6e 66 69   ^
00a0  67 2e 65 64 67 65 2e 73  6b 79 70 65 2e 63 6f 6d  g.edge.s
```

4. Decrypt TLS Traffic

- In Edit > Preferences > Protocols > TLS, set the pre-master secret log file name to the provided keys file.
- Decrypt TLS traffic using the captured keys.



Transport Layer Security

RSA keys list [Edit...]

TLS debug file [Browse...]

☑ Reassemble TLS records spanning multiple TCP segments

☑ Reassemble TLS Application Data spanning multiple TLS records

☐ Message Authentication Code (MAC), ignore "mac failed"

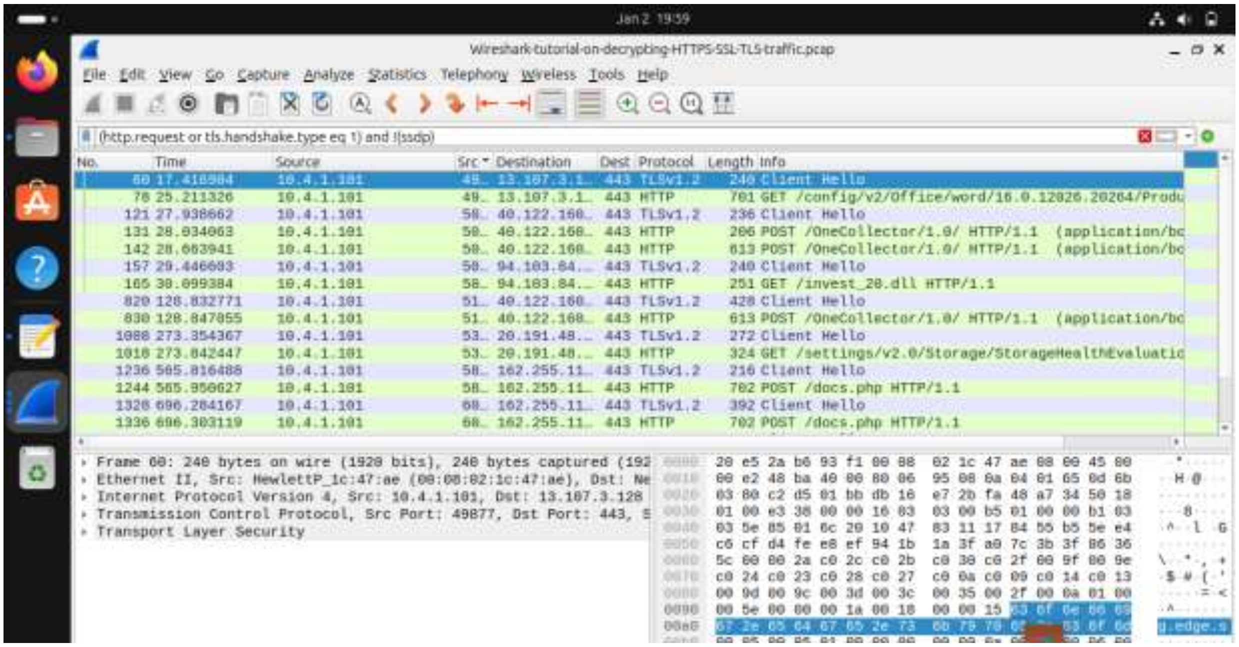
Pre-Shared Key

(Pre)-Master-Secret log filename

L-TLS-traffic/Wireshark-tutorial-KeysLogFile.txt [Browse...]

5. Identify Malicious Activity

- Construct a filter to display HTTP requests and TLS handshakes while excluding SSDP traffic.



Jan 2 19:59
Wireshark-tutorial-on-decrypting-HTTPS-SSL-TLS-traffic.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
(http.request or tls.handshake.type eq 1) and !(ssdp)
```

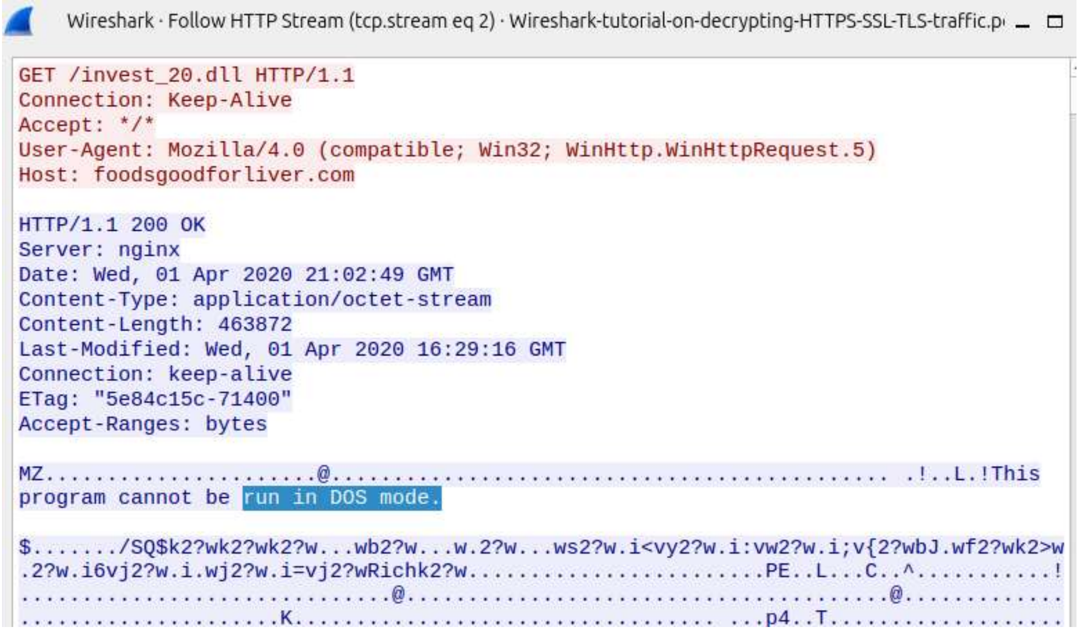
```
No.   Time        Source       Src▾ Destination    Dest Protocol Length Info
  60 17.418984   10.4.1.101   49.. 13.107.3.1..   443  TLSv1.2  240 Client Hello
  78 25.211326   10.4.1.101   49.. 13.107.3.1..   443  HTTP     701 GET /config/v2/Office/word/16.0.12026.20264/Produ
 121 27.938662   10.4.1.101   58.. 40.122.160..   443  TLSv1.2  236 Client Hello
 131 28.034063   10.4.1.101   58.. 40.122.160..   443  HTTP     206 POST /OneCollector/1.0/ HTTP/1.1  (application/bc
 142 28.083941   10.4.1.101   58.. 40.122.160..   443  HTTP     613 POST /OneCollector/1.0/ HTTP/1.1  (application/bc
 157 29.446603   10.4.1.101   58.. 94.103.84...   443  TLSv1.2  240 Client Hello
 165 30.099384   10.4.1.101   58.. 94.103.84...   443  HTTP     251 GET /invest_20.dll HTTP/1.1
 820 128.832771  10.4.1.101   51.. 40.122.160..   443  TLSv1.2  428 Client Hello
 830 128.847855  10.4.1.101   51.. 40.122.160..   443  HTTP     613 POST /OneCollector/1.0/ HTTP/1.1  (application/bc
1008 273.354367  10.4.1.101   53.. 20.191.48...   443  TLSv1.2  272 Client Hello
1018 273.842447  10.4.1.101   53.. 20.191.48...   443  HTTP     324 GET /settings/v2.0/Storage/StorageHealthEvaluatic
1236 565.816488  10.4.1.101   58.. 162.255.11..   443  TLSv1.2  216 Client Hello
1244 565.950627  10.4.1.101   58.. 162.255.11..   443  HTTP     702 POST /docs.php HTTP/1.1
1328 696.284167  10.4.1.101   60.. 162.255.11..   443  TLSv1.2  392 Client Hello
1336 696.303119  10.4.1.101   60.. 162.255.11..   443  HTTP     702 POST /docs.php HTTP/1.1
```

```
▸ Frame 60: 240 bytes on wire (1920 bits), 240 bytes captured (192
▸ Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Ne
▸ Internet Protocol Version 4, Src: 10.4.1.101, Dst: 13.107.3.128
▸ Transmission Control Protocol, Src Port: 49877, Dst Port: 443, S
▸ Transport Layer Security
```

```
0000  20 e5 2a b6 93 f1 00 08  02 1c 47 ae 08 00 45 00
0010  00 e2 48 ba 40 00 80 06  95 08 0a 04 01 65 0d 6b
0020  03 80 c2 d5 01 bb db 16  e7 2b fa 48 a7 34 50 18
0030  01 00 e3 38 00 00 16 03  03 00 b5 01 00 00 b1 03
0040  03 5e 85 01 6c 20 10 47  83 11 17 84 55 b5 5e e4
0050  c6 cf d4 fe e8 ef 94 1b  1a 3f a0 7c 3b 3f 86 36
0060  5c 00 00 2a c0 2c c0 2b  c0 30 c0 2f 00 9f 00 9e
0070  c0 24 c0 23 c0 28 c0 27  c0 0a c0 09 c0 14 c0 13
0080  00 9d 00 9c 00 3d 00 3c  00 35 00 2f 00 0a 01 00
0090  00 5e 00 00 00 1a 00 18  00 00 15 63 6f 6e 66 69
00a0  67 2e 65 64 67 65 2e 73  6b 79 70 [illegible] [illegible] 63 6f 6d   g.edge.s
```

6. Analyze Malicious Activity

- Analyze the requests to identify a suspicious DLL (invest20.dll).

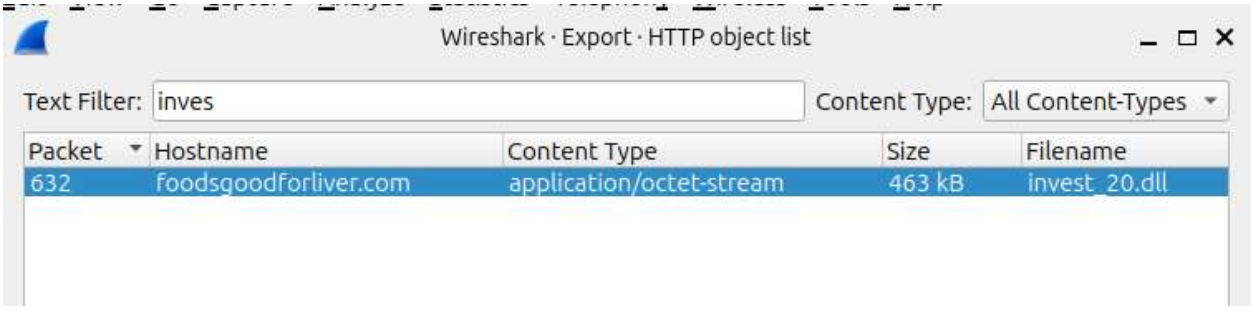


Wireshark · Follow HTTP Stream (tcp.stream eq 2) · Wireshark-tutorial-on-decrypting-HTTPS-SSL-TLS-traffic.p

```
GET /invest_20.dll HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
Host: foodsgoodforliver.com

HTTP/1.1 200 OK
Server: nginx
Date: Wed, 01 Apr 2020 21:02:49 GMT
Content-Type: application/octet-stream
Content-Length: 463872
Last-Modified: Wed, 01 Apr 2020 16:29:16 GMT
Connection: keep-alive
ETag: "5e84c15c-71400"
Accept-Ranges: bytes

MZ......................@.......................................... .!..L.!This
program cannot be run in DOS mode.

$......./SQ$k2?wk2?wk2?wk2?w...wb2?w...w.2?w...ws2?w.i<vy2?w.i:vw2?w.i;v{2?wbJ.wf2?wk2>w
.2?w.i6vj2?w.i.wj2?w.i=vj2?wRichk2?w......................PE..L...C..^...........!
..............................@........................................@............
.....................K................................ ...p4..T...................
```

7. Export Malicious Object

- Right-click on the packet corresponding to the DLL request and follow the HTTP stream.
- Use Wireshark's export objects feature to export the DLL object.



Wireshark · Export · HTTP object list

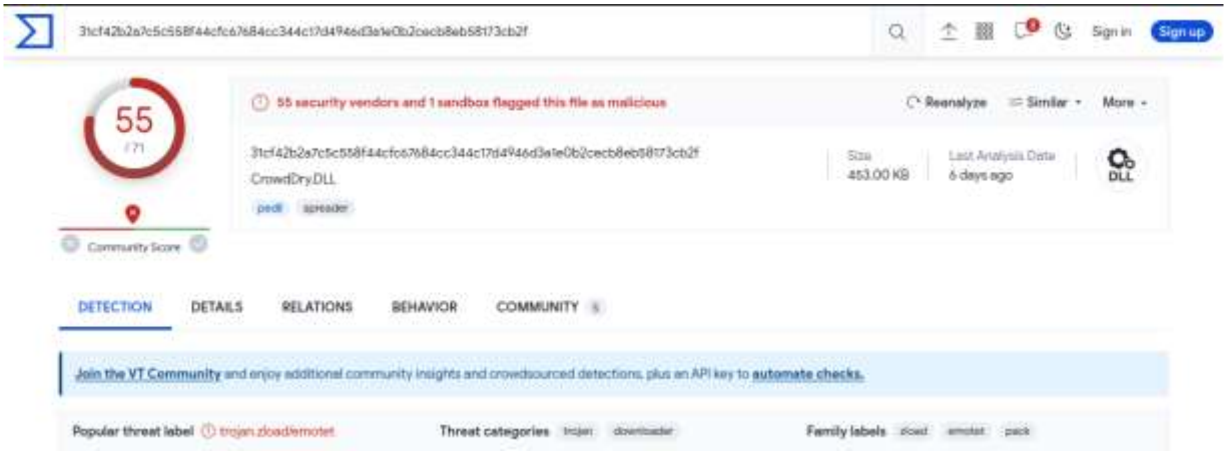
Text Filter: inves

Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
632	foodsgoodforliver.com	application/octet-stream	463 kB	invest_20.dll

8. Analyze Malware with VirusTotal

- Upload the exported DLL to VirusTotal for in-depth malware analysis.
- Identify the malware type (Drydex) and gather information on its behavior.



31cf42b2a7c5c558f44cfc67684cc344c17d4946d3a1e0b2cecb8eb58173cb2f

55 / 71

55 security vendors and 1 sandbox flagged this file as malicious

31cf42b2a7c5c558f44cfc67684cc344c17d4946d3a1e0b2cecb8eb58173cb2f

CrowdDry.DLL

peexe spreader

Size 453.00 KB

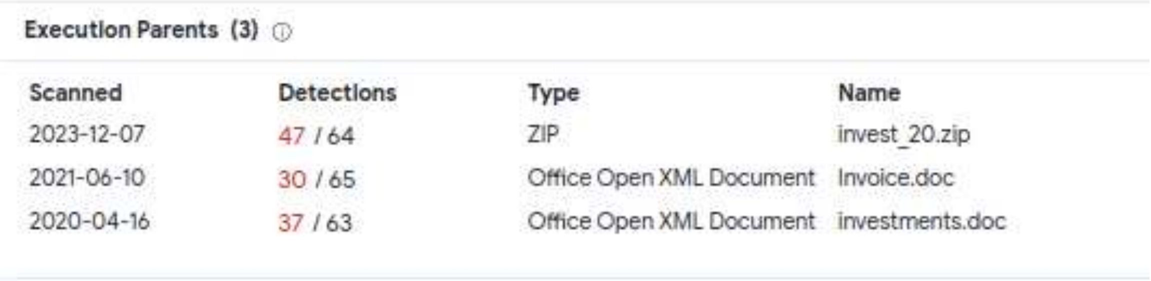
Last Analysis Date 6 days ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.zload/emotet

Threat categories trojan downloader

Family labels zload emotet pack



Execution Parents (3)

Scanned	Detections	Type	Name
2023-12-07	47 / 64	ZIP	invest_20.zip
2021-06-10	30 / 65	Office Open XML Document	Invoice.doc
2020-04-16	37 / 63	Office Open XML Document	investments.doc

Disclaimer and Ethical Considerations

The materials in this repository are intended for educational purposes related to network analysis. Users and contributors are expected to conduct their activities ethically, ensuring the utmost respect for privacy and adherence to legal standards. It is crucial to exercise responsible and lawful behavior when analyzing network data, refraining from the disclosure of sensitive information and maintaining a commitment to upholding ethical standards throughout the exploration and sharing of findings.