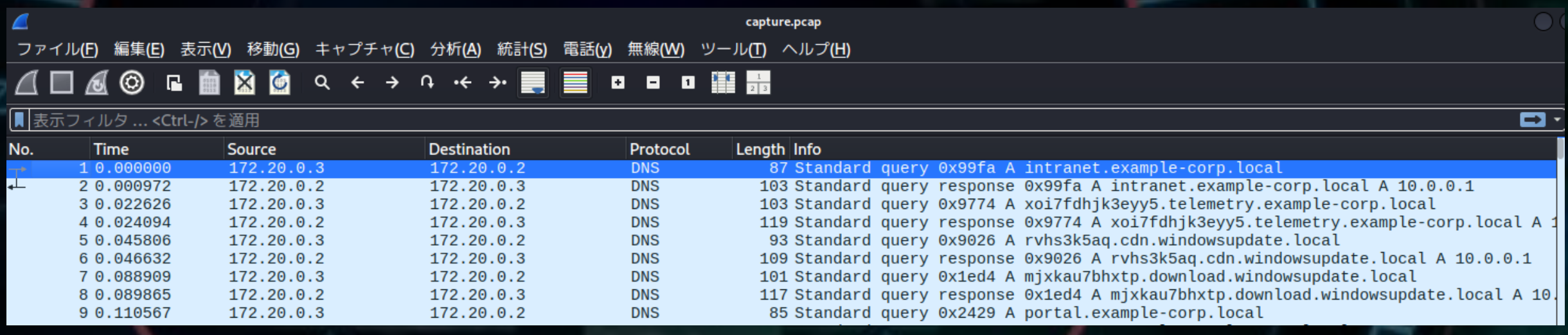
怪しい名前解決
解　説

添付ファイルの capture.pcap

ファイルをダウンロードし、

Wiresharkで開き確認します。



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.20.0.3	172.20.0.2	DNS	87	Standard query 0x99fa A intranet.example-corp.local
2	0.000972	172.20.0.2	172.20.0.3	DNS	103	Standard query response 0x99fa A intranet.example-corp.local A 10.0.0.1
3	0.022626	172.20.0.3	172.20.0.2	DNS	103	Standard query 0x9774 A xoi7fdhjk3eyy5.telemetry.example-corp.local
4	0.024094	172.20.0.2	172.20.0.3	DNS	119	Standard query response 0x9774 A xoi7fdhjk3eyy5.telemetry.example-corp.local A 1
5	0.045806	172.20.0.3	172.20.0.2	DNS	93	Standard query 0x9026 A rvhs3k5aq.cdn.windowsupdate.local
6	0.046632	172.20.0.2	172.20.0.3	DNS	109	Standard query response 0x9026 A rvhs3k5aq.cdn.windowsupdate.local A 10.0.0.1
7	0.088909	172.20.0.3	172.20.0.2	DNS	101	Standard query 0x1ed4 A mjxkau7bhxtp.download.windowsupdate.local
8	0.089865	172.20.0.2	172.20.0.3	DNS	117	Standard query response 0x1ed4 A mjxkau7bhxtp.download.windowsupdate.local A 10.
9	0.110567	172.20.0.3	172.20.0.2	DNS	85	Standard query 0x2429 A portal.example-corp.local

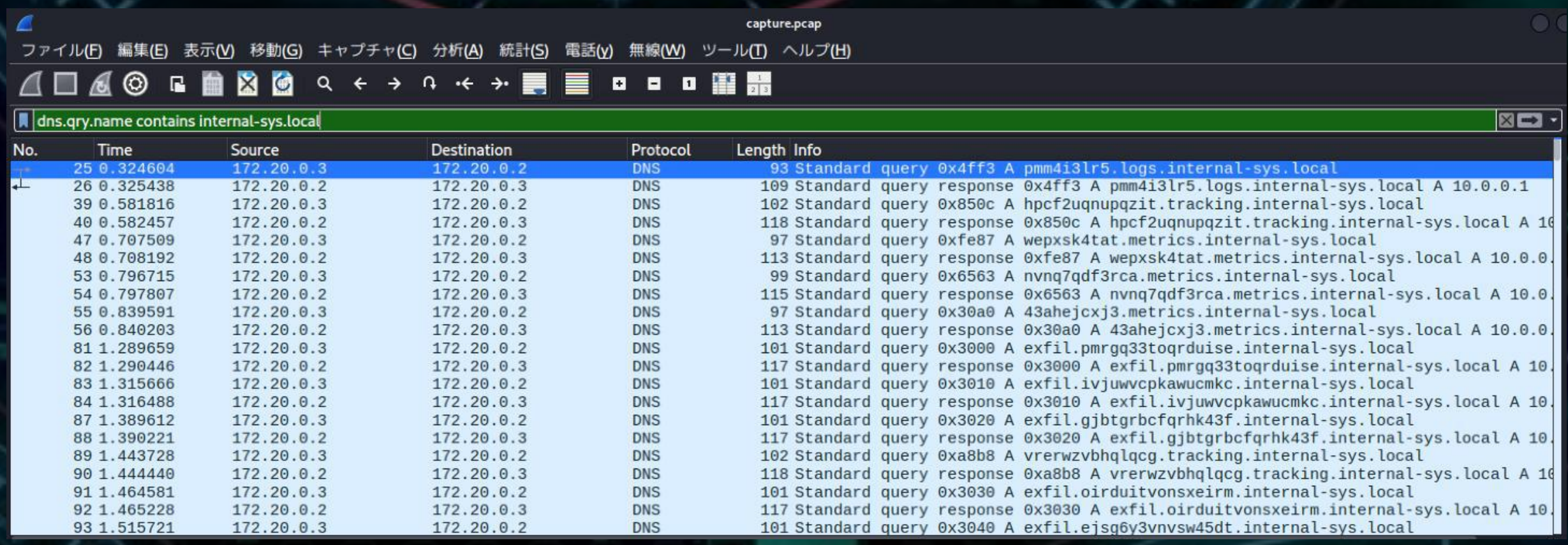
大量のDNSクエリが記録されています。

全てのパケットを確認すると、334件

のDNSのパケットが確認できます

クエリ先のドメインを確認すると、windowsupdate.local、microsoft.local、example-corp.localなど様々なドメインがある中で、internal-sys.localというドメインへのクエリが目立ちます。
internal-sys.local というドメインを抽出するために以下のクエリで検索をします。

```
dns.qry.name contains internal-sys.local
```



添付ファイルの capture.pcap ファイルをダウンロードし、Wiresharkで開き確認します。

次のドメインが確認でき、パケット数を確認すると以下の通りとなります。

- *.tracking.internal-sys.local：16パケット
- *.logs.internal-sys.local：4パケット
- *.metrics.internal-sys.local：16パケット
- exfil.*.internal-sys.local：132パケット

exfil.*.internal-sys.local がパケット数が多いため、以下のクエリで検索します。

```
dns.qry.name contains exfil
```

```
Info
Standard query 0x3000 A exfil.pmrgq33toqrduise.internal-sys.local
Standard query response 0x3000 A exfil.pmrgq33toqrduise.internal-sys.local A 10.0.0.1
Standard query 0x3010 A exfil.ivjuwvcpkawucmkc.internal-sys.local
Standard query response 0x3010 A exfil.ivjuwvcpkawucmkc.internal-sys.local A 10.0.0.1
Standard query 0x3020 A exfil.gjbtgrbcfqrhk43f.internal-sys.local
Standard query response 0x3020 A exfil.gjbtgrbcfqrhk43f.internal-sys.local A 10.0.0.1
Standard query 0x3030 A exfil.oirduitvonsxeirm.internal-sys.local
Standard query response 0x3030 A exfil.oirduitvonsxeirm.internal-sys.local A 10.0.0.1
Standard query 0x3040 A exfil.ejsg6y3vnvsw45dt.internal-sys.local
Standard query response 0x3040 A exfil.ejsg6y3vnvsw45dt.internal-sys.local A 10.0.0.1
Standard query 0x3050 A exfil.ei5fwisdhjofyvlt.internal-sys.local
Standard query response 0x3050 A exfil.ei5fwisdhjofyvlt.internal-sys.local A 10.0.0.1
Standard query 0x3060 A exfil.mvzhgxc4ovzwk4s4.internal-sys.local
Standard query response 0x3060 A exfil.mvzhgxc4ovzwk4s4.internal-sys.local A 10.0.0.1
Standard query 0x3070 A exfil.lrcg6y3vnvsw45dt.internal-sys.local
Standard query response 0x3070 A exfil.lrcg6y3vnvsw45dt.internal-sys.local A 10.0.0.1
Standard query 0x3080 A exfil.lrofaylton3w64te.internal-sys.local
Standard query response 0x3080 A exfil.lrofaylton3w64te.internal-sys.local A 10.0.0.1
Standard query 0x3090 A exfil.omxhq3dtparcyisd.internal-sys.local
Standard query response 0x3090 A exfil.omxhq3dtparcyisd.internal-sys.local A 10.0.0.1
Standard query 0x30a0 A exfil.hjofyvltmvzhgxc4.internal-sys.local
Standard query response 0x30a0 A exfil.hjofyvltmvzhgxc4.internal-sys.local A 10.0.0.1
```

exfil以降にランダムな文字列が確認出来ます。この文字列を抽出するため、以下のコマンドでAレコードのドメインを出力します。

```
tshark -r capture.pcap -Y 'dns.qry.name contains "exfil"' -T fields -e dns.qry.name
```

```
┌──(kali㉿kali)-[~/CTF/dns-tunnel-traffic/dist]
└─$ tshark -r capture.pcap -Y 'dns.qry.name contains "exfil"' -T fields -e dns.qry.name
exfil.pmrgq33toqrduise.internal-sys.local
exfil.pmrgq33toqrduise.internal-sys.local
exfil.ivjuwvcpkawucmkc.internal-sys.local
exfil.ivjuwvcpkawucmkc.internal-sys.local
exfil.gjbtgrbcfqrhk43f.internal-sys.local
```

リクエストパケットとレスポンスパケットが含まれるため、重複して表示されて
います。リクエストパケットのみ表示することで、重複を排除します。
以下の抽出コマンドで試します。

```
  tshark -r capture.pcap -Y 'dns.qry.name contains "exfil" and ip.src == 172.20.0.2' -T fields -e dns.qry.name
```

```
┌──(kali㉿kali)-[~/CTF/dns-tunnel-traffic/dist]
└─$ tshark -r capture.pcap -Y 'dns.qry.name contains "exfil" and ip.src == 172.20.0.2' -T fields -e dns.qry.name
exfil.pmrgq33toqrduise.internal-sys.local
exfil.ivjuwvcpkawucmkc.internal-sys.local
exfil.gjbtgrbcfqrhk43f.internal-sys.local
exfil.oirduitvonsxeirm.internal-sys.local
exfil.ejsg6y3vnvsw45dt.internal-sys.local
exfil.ei5fwisdhjofyvlt.internal-sys.local
exfil.mvzhgxc4ovzwk4s4.internal-sys.local
```

正規表現でexfil以降の文字列を抽出します。以下のコマンドで正規表現
を用いて抽出できます。

```
  tshark -r capture.pcap -Y 'dns.qry.name contains "exfil" and ip.src == 172.20.0.2' -T fields -e dns.qry.name | grep -Eo 'exfil.[^¥.]+' | grep -Eo '[^¥.]+$'
```

```
┌──(kali㉿kali)-[~/CTF/dns-tunnel-traffic/dist]
└─$ tshark -r capture.pcap -Y 'dns.qry.name contains "exfil" and ip.src == 172.20.0.2' -T fields -e dns.qry.name | grep -Eo 'exfil.[^.\]+' | grep -Eo '[^\.]+$'
pmrgq33toqrduise
ivjuwvcpkawucmkc
gjbtgrbcfqrhk43f
oirduitvonsxeirm
ejsg6y3vnvsw45dt
ei5fwisdhjofyvlt
```

抽出に成功しました。これらのサブドメイン部分の文字の出現はアルファベットや数字はどこからどこまでの範囲であるか、以下のコマンドで調査出来ます。

```
tshark -r capture.pcap -Y 'dns.qry.name contains "exfil" and ip.src == 172.20.0.2' -T fields -e dns.qry.name | grep -Eo 'exfil.[^¥.]+' | grep -Eo '[^¥.]+$' | grep -o . | sort -u
```

```
┌──(kali㉿kali)-[~/CTF/dns-tunnel-traffic/dist]
└─$ tshark -r capture.pcap -Y 'dns.qry.name contains "exfil" and ip.src == 172.20.0.2' -T fields -e dns.qry.name | grep -Eo 'exfil\.[^.]+' | grep -Eo '[^.]+$' | grep -o . | sort -u

2
3
4
5
6
7
a
b
c
d
e
f
g
h
i
j
k
l
m
n
o
p
q
r
s
t
u
v
w
x
y
z
```

調査の結果、2-7, a-z の文字のみを使用して記載されていることがわかります。
このルールはbase32でエンコードした際に生じるものです。全てのサブドメインを連結することで、base32形式でデコード出来ると推測されます。ただし、base32エンコードでは、大文字を使用します。連結後に小文字を大文字に変換してからデコーダーに送る必要があります。

以下のコマンドにてtrコマンドを用いて改行を削除し連結し、小文字を大文字に変換してからbase32でデコードします。

```
tshark -r capture.pcap -Y 'dns.qry.name contains "exfil" and ip.src == 172.20.0.2' -T fields -e dns.qry.name | grep -Eo 'exfil.[^¥.]+' | grep -Eo '[^¥.]+$' | tr -d '¥n' | tr 'a-z' 'A-Z' | base32 -d
```

```
┌──(kali㉿kali)-[~/CTF/dns-tunnel-traffic/dist]
└─$ tshark -r capture.pcap -Y 'dns.qry.name contains "exfil" and ip.src == 172.20.0.2' -T fields -e dns.qry.name | grep -Eo 'exfil\.[^.]+
' | grep -Eo '[^.]+$' | tr -d '\n' | tr 'a-z' 'A-Z' | base32 -d
{"host":"DESKTOP-A1B2C3D","user":"user","documents":["C:\\Users\\user\\Documents\\Passwords.xlsx","C:\\Users\\user\\Documents\\社外秘_顧客リスト.xlsx","C:\\Users\\user\\Documents\\VPN_credentials.txt","C:\\Users\\user\\Documents\\flag{dn5_tunn3l_3xf1l}.txt","C:\\Users\\user\\Documents\\人事評価_2024.docx"],"chrome":{"login_data":"C:\\Users\\user\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Login Data","cookies":"C:\\Users\\user\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Cookies","history":"C:\\Users\\user\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\History"},"system":{"os":"Windows 10 Pro","domain":"CORP.LOCAL"}}
```

フラグが取得出来ました。

flag{dn5_tunn3l_3xf1l}