Litter Challenge

Sherlock Scenario
Khalid has just logged onto a host that he and his team use as a testing host for many different purposes. It's off their corporate network but has access to lots of resources on the network. The host is used as a dumping ground for a lot of people at the company, but it's very useful, so no one has raised any issues. Little does Khalid know; the machine has been compromised and company information that should not have been on there has now been stolen – it's up to you to figure out what has happened and what data has been taken.

Task 1:
At a glance, what protocol seems to be suspect in this attack?

While opening the pcap file, I first saw a lot of DNS packets so I assumed it will be DNS

16	2023-04-30 10:26:57.656217	192.168.157.144	55817	192.168.157.2	53	DNS
17	2023-04-30 10:26:57.668309	192.168.157.144	50942	192.168.157.2	53	DNS
18	2023-04-30 10:26:57.670226	192.168.157.144	58045	192.168.157.2	53	DNS
19	2023-04-30 10:26:57.672321	192.168.157.144	59254	192.168.157.2	53	DNS
20	2023-04-30 10:26:57.673380	192.168.157.144	62909	192.168.157.2	53	DNS
21	2023-04-30 10:26:57.675436	192.168.157.144	59935	192.168.157.2	53	DNS
22	2023-04-30 10:26:57.676399	192.168.157.144	63618	192.168.157.2	53	DNS
23	2023-04-30 10:26:57.677497	192.168.157.144	58959	192.168.157.2	53	DNS
24	2023-04-30 10:26:57.678019	192.168.157.144	56349	192.168.157.2	53	DNS
25	2023-04-30 10:26:57.678212	192.168.157.2	53	192.168.157.144	52849	DNS
26	2023-04-30 10:26:57.687263	192.168.157.2	53	192.168.157.144	55817	DNS
27	2023-04-30 10:26:57.696000	192.168.157.2	53	192.168.157.144	50942	DNS
28	2023-04-30 10:26:57.702147	192.168.157.2	53	192.168.157.144	58045	DNS
29	2023-04-30 10:26:57.703812	192.168.157.2	53	192.168.157.144	59935	DNS
30	2023-04-30 10:26:57.705983	192.168.157.2	53	192.168.157.144	62909	DNS
31	2023-04-30 10:26:57.708654	192.168.157.2	53	192.168.157.144	59254	DNS
32	2023-04-30 10:26:57.709302	192.168.157.2	53	192.168.157.144	58959	DNS
33	2023-04-30 10:26:57.712348	192.168.157.2	53	192.168.157.144	63618	DNS
34	2023-04-30 10:26:57.729221	192.168.157.2	53	192.168.157.144	56349	DNS

Answer: DNS

Task 2:
There seems to be a lot of traffic between our host and another, what is the IP address of the suspect host?

I checked the conversation and filtered by the packets

Ethernet · 18 | IPv4 · 244 | IPv6 · 3 | TCP · 363 | UDP · 986

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.157.144	192.168.157.145	10,901	2 MB	5,451	1 MB	5,450	1 MB	149.557152	2068.1893	4144 bits/s	5069 bits/s
192.168.157.144	173.194.129.201	7,024	8 MB	794	90 kB	6,230	8 MB	566.695641	201.5394	3554 bits/s	313 kbps

Answer: 192.168.157.145

Task 3:
What is the first command the attacker sends to the client?

I filtered for ip.addr == 192.168.157.145 and followed the UDP Stream

Wireshark · Follow UDP Stream (udp.stream eq 481) · suspicious_traffic.pcap

```
3...........<6bea0068813566002163 6f6d6d616e6420284445534b544f502d554d4e43
4245372900
microsofto365.com.....3...........<6bea0068813566002163 6f6d6d616e6420284445534b544f502d554d4e43
4245372900
microsofto365.com..............<.(.
.60da0068813b4fc0000
microsofto365.com.'m...........4f3201688135 66b4fc
microsofto365.com.....'m...........4f3201688135 66b4fc
microsofto365.com..............<.(.
.ff4b016881b4fc3566
microsofto365.com.6............6f7301688135 66b4fc
microsofto365.com.....6............6f7301688135 66b4fc
microsofto365.com..............<...59a3016881b4fc3566*............17f601688135 66b4fc
microsofto365.com.....*............17f601688135 66b4fc
microsofto365.com..............<.(.
.b23b016881b4fc3566
microsofto365.com..............3f1a01688135 66b4fc
microsofto365.com..............3f1a01688135 66b4fc
microsofto365.com..............<.(.
.bba1016881b4fc3566
microsofto365.com..............288401688135 66b4fc
microsofto365.com..............288401688135 66b4fc
microsofto365.com..............<.(.
.8a99016881b4fc3566
microsofto365.com.%............62ad01688135 66b4fc
microsofto365.com.....%............62ad01688135 66b4fc
microsofto365.com..............<.(.
.5f0701688 1b4fc3566
microsofto365.com.x............300401688135 66b4fc
microsofto365.com.....x............300401688135 66b4fc
microsofto365.com..............<.(.
```

Then I copied everything and paste it inside CyberChef and used the "From Hex" recipe

Input

```
microsofto365.com..............<...6986011ccd781b4c5d".............4578011ccd4c5d781b
microsofto365.com....."............4578011ccd4c5d781b
microsofto365.com..............<.&.5da7011ccd781b4c5d
microsofto365.com.#............1a26011ccd4c5d781b
microsofto365.com.....#............1a26011ccd4c5d781b
microsofto365.com..............<...ce8a011ccd781b4c5d.............0922011ccd4c5d781b
microsofto365.com.................0922011ccd4c5d781b
microsofto365.com..............<.(.
.a213011ccd781b4c5d
microsofto365.com.]............4fdb011ccd4c5d781b
microsofto365.com.....]............4fdb011ccd4c5d781b
microsofto365.com..............<.(.
.a666011ccd781b4c5d
microsofto365.com.99...........3706011ccd4c5d781b
microsofto365.com.....99...........3706011ccd4c5d781b
microsofto365.com..............<.(.
.0912011ccd781b4c5d
microsofto365.com..............253c011ccd4c5d781b
microsofto365.com.................253c011ccd4c5d781b
microsofto365.com..............<.&.9cb7011ccd781b4c5d
microsofto365.com.I............59b8011ccd4c5d781b
microsofto365.com.....I............59b8011ccd4c5d781b
microsofto365.com..............<.(.
.aba3011ccd781b4c5d
microsofto365.com.x............3e85011ccd4c5d781b
microsofto365.com.....x............3e85011ccd4c5d781b
microsofto365.com..............<.&.fa28011ccd781b4c5d
microsofto365.com.
```

1854113 15073

Output

```
î\SOHh•µLF5p
STX ENQ
>äSOH FS ÍA`u!
STX ENQ
>äSOH FS ÍA`u!
STX ENQ
ç÷SOH FS Íu!A`whoamiLF ^6SOH FS ÍA`u(whoamiLFdesktop-umncbe7\testCR LF CR LFC:\Users\test\Downloads>
STX ENQ
^6SOH FS ÍA`u(whoamiLFdesktop-umncbe7\testCR LF CR LFC:\Users\test\Downloads>
```

Answer: whoami

Task 4:
What is the version of the DNS tunneling tool the attacker is using?

I scrolled down the output and found the version

```
IØSOH FS ÍD0u,B.Browser.for.SQLite-3.12.2-win64.msiCR LF28/05/2016  21:38          142,336 dnscat2-v0.07-client
STX ENQ
IØSOH FS ÍD0u,B.Browser.for.SQLite-3.12.2-win64.msiCR LF28/05/2016  21:38          142,336 dnscat2-v0.07-client
```

Answer: 0.07

Task 5:
The attackers attempts to rename the tool they accidentally left on the clients host. What do they name it to?

I downloaded the output from CyberChef and opened notepad++ and searched for "dnscat2-v0.07"

```
5pFFST6ENQFFgçSOHFSÞeu‘FFST6ENQFFgçSOHFSÞeu‘FFST6ENQFFNAR=SOHFSu‘Peren dnscat2-v0.07-clieACKmB’v-†"3↑W†RBEIv-7π-¥1FSYNW"↑W†P
FFST6ENQFF^SOHFSÞeuŗen dnscat2-v0.07-client-win32.exe win installer.ext†P ◘3¥|W6W'5ŗW7EFþv1↑SYN33SOHFFST6ENQFF^SOHFSÞeuŗen dnscat2-v0.07-client-win32.exe win installer.ext†P ◘3¥|W6W'5ŗW7EFþv
```

Answer: win_installer.exe

Task 6:
The attacker attempts to enumerate the users cloud storage. How many files do they locate in their cloud storage directory?

I scrolled down until I found OneDrive with some output of 0 file and 0 bytes and also DIR command

```
SOH VT SOH FS IuO\Ecd OneDriveLF ACK ETX äSOH FS I\Euàcd OneDriveLF CR LFC:\Users\test\OneDrive>
STX ENQ
ACK ETX äSOH FS Í\Èuàcd OneDriveLF CR LFC:\Users\test\OneDrive>
STX ENQ
úrSOH FS Íuà\ídirLF )ESOH FS Í\íuädirLF  Volume in drive C has no label.CR LF  Volume Serial Number is 503A-D127CR LF CR LF  Directory of C:\Us
STX ENQ
)ESOH FS Í\íuädirLF  Volume in drive C has no label.CR LF  Volume Serial Number is 503A-D127CR LF CR LF  Directory of C:\Us
STX ENQ
¿ SOH FS Íuä]L
STX ENQ
BELÒSOH FS Í]Luäers\test\OneDriveCR LF CR LF04/06/2021  08:52    <DIR>          .CR LF04/06/2021  08:52    <DIR>
STX ENQ
BELÒSOH FS Í]Luäers\test\OneDriveCR LF CR LF04/06/2021  08:52    <DIR>          .CR LF04/06/2021  08:52    <DIR>
STX ENQ
É•SOH FS Íuä]«
STX ENQ
FS •SOH FS Í]«uä ..CR LF               0 File(s)              0 bytesCR LF               2 Dir(s)  24,470,171,648 byt
STX ENQ
FS •SOH FS Í]«uä ..CR LF               0 File(s)              0 bytesCR LF               2 Dir(s)  24,470,171,648 byt
```

Answer: 0

Task 7:
What is the full location of the PII file that was stolen?

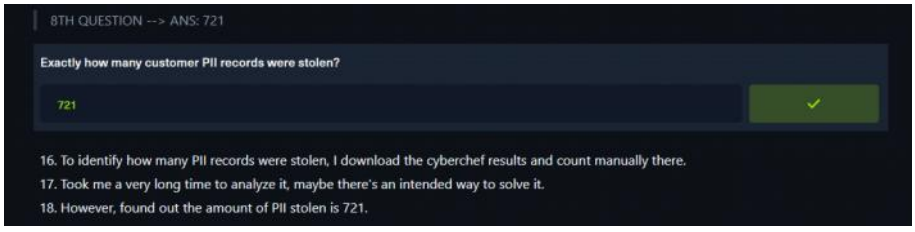
I kept scrolling down until I found some path which I assumed related to this task

```
§ LF SOH FS Íwb•8type "C:\Users\test\DoACK7VÖVçG5Æ6Æ•VçBACKFETBFDC1ACK+±±LF•Ö•6ETBF•Ö SO \user details.csv" LF
SI 6ENQ
qpSOH FS Í•8w«type "C:\Users\test\Documents\client data optimisation\user details.csv" LF ,job,company,ssn,resid
SI 6ENQ
qpSOH FS Í•8w«type "C:\Users\test\Documents\client data optimisation\user details.csv" LF ,job,company,ssn,resid
```

Answer: C:\users\test\documents\client data optimisation\user details.csv

Task 8:
Exactly how many customer PII records were stolen?

I used the write-up for this task



Answer: 721n