1.Fase de análisis y descripción de pcaps minados

In [1]:
```
import pandas as pd
```

En esta fase se realizará la extracción de los pcaps necesarios para nuestra investigación. Las **actividades** son:

```
a.    Obtener una muestra de capturas de tráfico de red de ataques de botnets para s
u posterior análisis
```

En esta fase, nuestros **entregables** son:

1. Conjunto de pcaps estructurados en benignos y malignos
2. Análisis preliminar de los pcaps, detallando fuentes de extracción y herramientas utilizadas para ello

Entregables

Fuentes de extracción

Se procedio a la descarga de una serie de pcaps provistos por el laboratorio https://www.stratosphereips.org/

1. Benignos

In [2]:
```
s_benigns = pd.read_csv(r"C:\Users\Usuario\Documents\Github\PDG\PDG-2\PCAPS\Information about pcapc benigns
```

In [3]:
```
s_benigns
```

	Reference	Link	Pcap Name
0	1	https://mcfp.felk.cvut.cz/publicDatasets/CTU-N...	2017-05-02_normal
1	2	https://mcfp.felk.cvut.cz/publicDatasets/CTU-N...	2017-05-01_normal
2	3	https://mcfp.felk.cvut.cz/publicDatasets/CTU-N...	2017-05-01_normal(1)
3	4	https://mcfp.felk.cvut.cz/publicDatasets/CTU-N...	2017-05-01_normal(2)
4	5	https://mcfp.felk.cvut.cz/publicDatasets/CTU-N...	2017-05-01_normal(3)
5	6	https://mcfp.felk.cvut.cz/publicDatasets/CTU-N...	2017-04-30_win-normal
6	7	https://mcfp.felk.cvut.cz/publicDatasets/CTU-N...	2017-04-28_normal
7	8	https://mcfp.felk.cvut.cz/publicDatasets/CTU-N...	2017-04-25_win-normal
8	9	https://mcfp.felk.cvut.cz/publicDatasets/CTU-N...	2017-04-19_win-normal
9	10	https://mcfp.felk.cvut.cz/publicDatasets/CTU-N...	2017-04-18_win-normal
10	11	https://mcfp.felk.cvut.cz/publicDatasets/CTU-N...	2017-05-02_kali-normal
11	12	https://mcfp.felk.cvut.cz/publicDatasets/CTU-N...	2017-05-02_kali-normal(1)
12	13	https://mcfp.felk.cvut.cz/publicDatasets/CTU-N...	2017_04_30-normal
13	14	https://mcfp.felk.cvut.cz/publicDatasets/CTU-N...	2017-07-03_capture-win2
14	15	https://mcfp.felk.cvut.cz/publicDatasets/CTU-N...	2013-12-17_capture1
15	16	https://mcfp.felk.cvut.cz/publicDatasets/CTU-N...	2013-12-17_capture1(1)
16	17	https://mcfp.felk.cvut.cz/publicDatasets/CTU-N...	2013-10-21_capture-1-only-dns
17	18	https://mcfp.felk.cvut.cz/publicDatasets/CTU-N...	2015-03-24_capture1-only-dns
18	19	Local Network (HTTP, Zoom, LOL, Youtube)	19
19	20	Local Network (HTTP, Zoom, LOL, Youtube)	20
20	21	Local Network (HTTP, Zoom, LOL, Youtube)	21
21	22	Local Network (HTTP, Zoom, LOL, Youtube)	22
22	23	Local Network (HTTP, Zoom, LOL, Youtube)	23
23	24	Local Network (HTTP, Zoom, LOL, Youtube)	24
24	25	Local Network (HTTP, Zoom, LOL, Youtube)	25
25	26	Local Network (HTTP, Zoom, LOL, Youtube)	26
26	27	Local Network (HTTP, Zoom, LOL, Youtube)	27
27	28	Local Network (HTTP, Zoom, LOL, Youtube)	28
28	29	Local Network (HTTP, Zoom, LOL, Youtube)	29
29	30	Local Network (HTTP, Zoom, LOL, Youtube)	30
30	31	Local Network (HTTP, Zoom, LOL, Youtube)	31
31	32	Local Network (HTTP, Zoom, LOL, Youtube)	32
32	33	Local Network (HTTP, Zoom, LOL, Youtube)	33
33	34	Local Network (HTTP, Zoom, LOL, Youtube)	34

34	35	Local Network (HTTP, Zoom, LOL, Youtube)	35
35	36	Local Network (HTTP, Zoom, LOL, Youtube)	36
36	37	Local Network (HTTP, Zoom, LOL, Youtube)	37
37	38	Local Network (HTTP, Zoom, LOL, Youtube)	38
38	39	Local Network (HTTP, Zoom, LOL, Youtube)	39
39	40	Local Network (HTTP, Zoom, LOL, Youtube)	40

---

2. Malignos

In [4]:
```
s_maligns = pd.read_csv(r"C:\Users\Usuario\Documents\Github\PDG\PDG-2\PCAPS\Information about pcaps Maligns
```

In [5]:
```
s_maligns
```

	Ref	Download	Pcap Name
0	1	https://mcfp.felk.cvut.cz/publicDatasets/CTU-M...	2018-05-03_win12
1	2	https://mcfp.felk.cvut.cz/publicDatasets/CTU-M...	162.222.213.28
2	3	https://mcfp.felk.cvut.cz/publicDatasets/CTU-M...	2018-04-04_win16
3	4	https://mcfp.felk.cvut.cz/publicDatasets/CTU-M...	2018-04-03_win12
4	5	https://mcfp.felk.cvut.cz/publicDatasets/CTU-M...	2018-04-03_win11
...	...	...	...
75	76	https://mcfp.felk.cvut.cz/publicDatasets/CTU-M...	2017-06-24_win8
76	77	https://mcfp.felk.cvut.cz/publicDatasets/CTU-M...	2017-06-24_win7
77	78	https://mcfp.felk.cvut.cz/publicDatasets/CTU-M...	2017-06-24_win6
78	79	https://mcfp.felk.cvut.cz/publicDatasets/CTU-M...	2017-06-24_win5
79	80	https://mcfp.felk.cvut.cz/publicDatasets/CTU-M...	2017-06-24_win4

80 rows × 3 columns