Pokročilé metódy grafickej analýzy komplexných dát

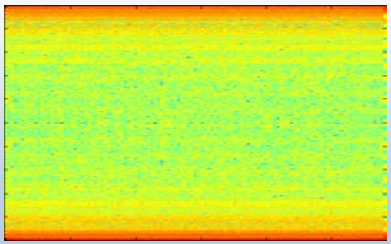
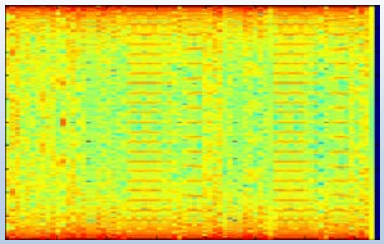
Ciele:

- Nekonvenčné metódy analýzy
- Detekcia škodlivého softvéru
- Využitie v sieťach
- Dynamický algoritmus

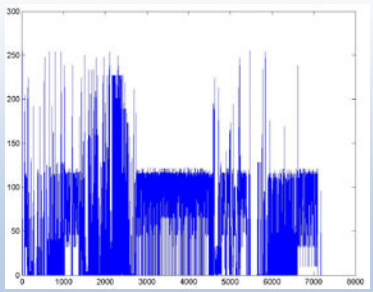
Využité metódy:

- Shannonova entropia
- Fourierove transformácie
- Vlnkové transformácie
- Štatistické metódy

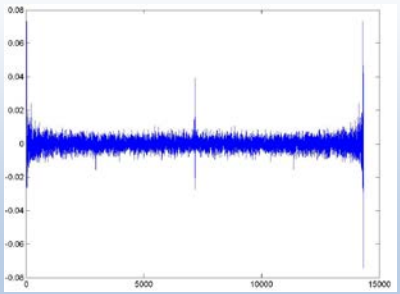
Krátkodobá Fourierova transformácia nad poľom entropie .jpg (ľavo) a .exe (pravo)

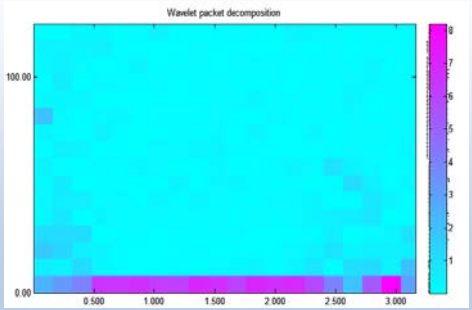
Hladina entropie binárneho súboru



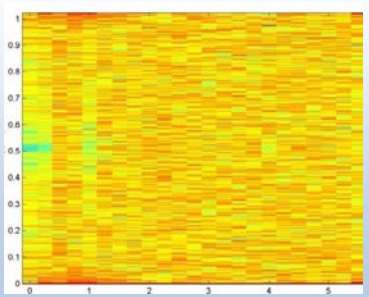
Frekvenčná analýza spustiteľného súboru



Vlnková transformácia



Metadáta .jpg súboru

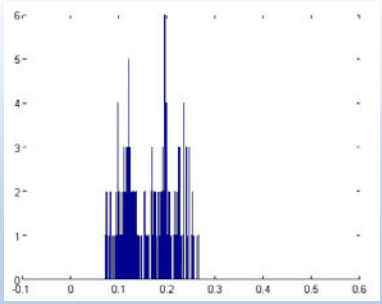
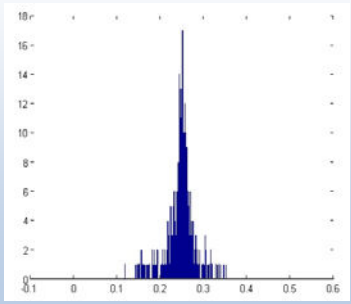


Autor: **Michal Chalupka**

Mentor: **doc. Ing. František Jakab, PhD.**

Konzultant: **Ing. Ivan Klimek**

Štatistické vyhodnocovanie pomocou histogramov

Dosiahnuté výsledky detekcie:

Typ súboru	Počet súborov	Prvá rovnica	MODEL MATCH	TRUE POSITIVE	FALSE POSITIVE	POSSIBLE MALWARE
Malware LEARN	2000	1160	768	96,4%	0%	768
Malware 1	2000	1073	531	80,2%	0%	787
Malware 2	2000	1086	549	81,75%	0%	792
EXE	691	0	0	0%	0%	591
JAR	273	0	0	0%	0%	28
DLL	414	0	0	0%	0%	321
JPG	674	0	0	0%	0%	178
PDF	812	0	0	0%	0%	10
DOC	356	0	0	0%	0%	320
MP3	100	0	0	0%	0%	6
XLS	244	0	0	0%	0%	244