Modul_27_2_10_Extract_an_Executable_from_a_PCAP

Part 1

f)
What are all those symbols shown in the Follow TCP Stream window? Are they connection noise? Data? Explain.

- Jelikož je to executable soubor, tak je to prostě co se stane po otevření binary souboru.

There are a few readable words spread among the symbols. Why are they there?

- co se dalo přeložit (co byl wireshark schopen konvertovat do textu)

Challenge Question: Despite the W32.Nimda.Amm.exe name, this executable is not the famous worm. For security reasons, this is another executable file that was renamed as W32.Nimda.Amm.exe. Using the word fragments displayed by Wireshark's Follow TCP Stream window, can you tell what executable this really is?

- asi CMD.exe of Microsoftu

```
%.........PZ.............j..h.......... o.............o.............P...
........I.D.I. .A.P.P.I.C.O.N...M.U.I.........<?xml version="1.0" encoding="UTF
standalone="yes"?>
<!-- Copyright (c) Microsoft Corporation -->
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
<assemblyIdentity
    version="5.1.0.0"
    processorArchitecture="amd64"
    name="Microsoft.Windows.FileSystem.CMD"
    type="win32"
/>
<description>Windows Command Processor</description>

<trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
    <security>
        <requestedPrivileges>
            <requestedExecutionLevel
                level="asInvoker"
                uiAccess="false"
            />
        </requestedPrivileges>
    </security>
</trustInfo>
<application  xmlns="urn:schemas-microsoft-com:asm.v3">
    <windowsSettings>
        <dpiAware  xmlns="http://schemas.microsoft.com/SMI/2005/
WindowsSettings">true</dpiAware>
    </windowsSettings>
</application>
</assembly>
```

Part 2

c)

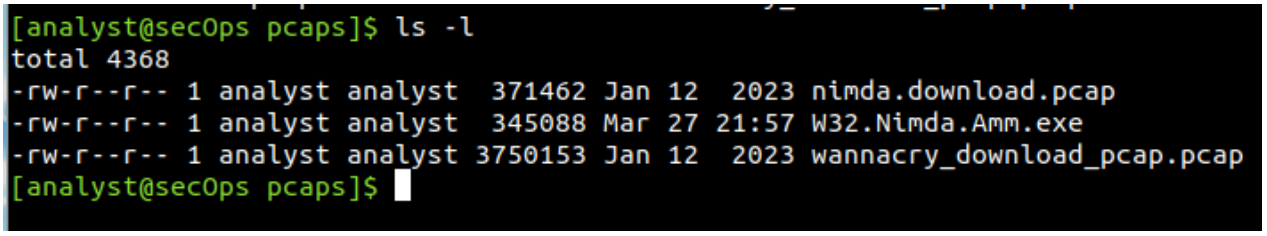
Why is W32.Nimda.Amm.exe the only file in the capture?

- pravděpodobně protože celé komunikace byla hlavně o tomto souboru a nic dalšího v komunikaci neproběhlo

f)

Was the file saved?

- ano



g)

In the malware analysis process, what would be a probable next step for a security analyst?

- další krok by byl nejlepší dát exe soubor do sandbox zařízení, odpíchnutý od všeho a tam soubor spustit a koukat se co přesně se děje se zařízením.