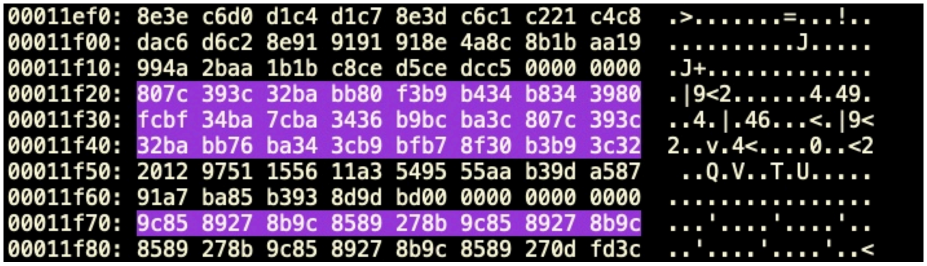
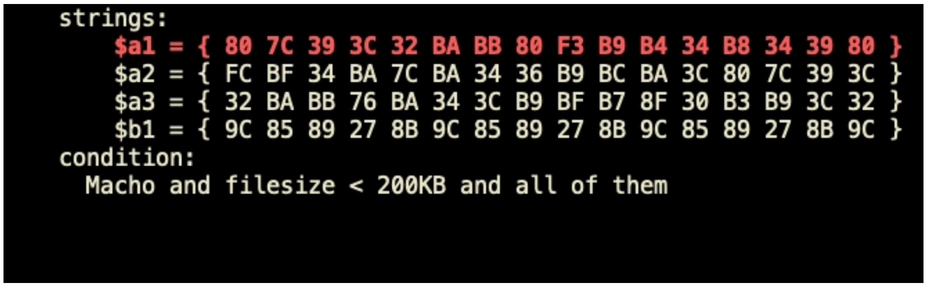
Unit #5

Malware Analysis

Malware	
Virus	● Malicious code that replicates itself on the computer. ● It has to be activated before it can spread.
Worms	● Malicious code that affects the computer. ● It is self-replicating and can email itself to others.
Trojan horse	● Malware is concealed within a seemingly useful program. The malware is executed once the program is run.
Ransomware	● Blocks access to assets until a sum is paid. ● It mainly targets government, education, banks, manufacturing, energy & utilities.

- **Blended threat -** combines multiple threats into one package. *Eg. using a trojan horse to sneak in a virus.*

Antivirus software - a type of program that prevents, detects, and eradicates malware.	
Malware signature	● Disables software with sequences of code typical to a specific piece of malware. ● It can only protect against known threats.  

```
00011ef0: 8e3e c6d0 d1c4 d1c7 8e3d c6c1 c221 c4c8  .>.......=...!..
00011f00: dac6 d6c2 8e91 9191 918e 4a8c 8b1b aa19  ..........J.....
00011f10: 994a 2baa 1b1b c8ce d5ce dcc5 0000 0000  .J+.............
00011f20: 807c 393c 32ba bb80 f3b9 b434 b834 3980  .|9<2......4.49.
00011f30: fcbf 34ba 7cba 3436 b9bc ba3c 807c 393c  ..4.|.46...<.|9<
00011f40: 32ba bb76 ba34 3cb9 bfb7 8f30 b3b9 3c32  2..v.4<....0..<2
00011f50: 2012 9751 1556 11a3 5495 55aa b39d a587   ..Q.V..T.U.....
00011f60: 91a7 ba85 b393 8d9d bd00 0000 0000 0000  ................
00011f70: 9c85 8927 8b9c 8589 278b 9c85 8927 8b9c  ...'....'....'..
00011f80: 8589 278b 9c85 8927 8b9c 8589 270d fd3c  ..'....'....'..<
```

```
    strings:
        $a1 = { 80 7C 39 3C 32 BA BB 80 F3 B9 B4 34 B8 34 39 80 }
        $a2 = { FC BF 34 BA 7C BA 34 36 B9 BC BA 3C 80 7C 39 3C }
        $a3 = { 32 BA BB 76 BA 34 3C B9 BF B7 8F 30 B3 B9 3C 32 }
        $b1 = { 9C 85 89 27 8B 9C 85 89 27 8B 9C 85 89 27 8B 9C }
    condition:
      Macho and filesize < 200KB and all of them
```

System monitoring	● The software can monitor a system's behavior. ● Atypical behavior is flagged. *Eg. unusually large increase in data usage, and attempts to access a large number of files.* ● Provides real-time protection.

Malware analysis	
Process isolation	● Process address spaces are separated to ensure other processes can't tamper with each other.
Virtual machine	● Simulates all aspects of a hardware device. ● Allows users to test how malware interacts with file systems, registry, etc. ● However, some malware can detect VMs and behave differently inside them. ● There is some risk of an escape attack.
Docker containers	● A package of software that includes everything needed to run an application. ● It provides isolation from host systems but there can still be a risk of an escape attack because the OS kernel is shared between containers and host.
Sandboxes	● Opens up files in a carefully isolated environment and observes the effects of the file. ● Threat actors can evade sandboxing by delaying malware execution because sandboxes typically run malware for a short time. Delaying it prevents the malware from exhibiting malicious behavior that the sandbox analyzes.

- **Forensic analysis -** analysis of digital evidence and investigation of security incidents.
  - Common artifacts include windows event logs, file metadata, deleted files, browser history, cookies, cache, download history, firewall logs, etc.

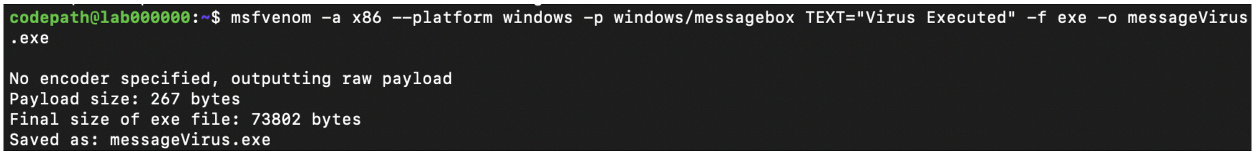
Network forensic analysis

- **PCAP -** a file that contains packet data.
  - Applications such as Wireshark are crucial to analyze pcaps.
- Forensic analysts have to ask questions such as:
  - What damage has been done?
  - Who was the perpetrator? How were the security measures passed?
  - Did the perpetrator leave anything behind such as a new account or malware?
  - Is there enough data to reproduce the attack and test it against a new control(s)?
- In order to properly identify suspicious network activities, there are reference files for standard network behaviors. *Eg. https://wiki.wireshark.org/samplecaptures*
- Suspicious activities include:

    - Unusual communication pairs (nodes that don't typically communicate suddenly are)
    - Unusual protocols and ports (understand what ports are open and active in the network. Unfamiliar open ports are suspicious)
    - Excessive failed connections
    - Suspicious inbound connections
- **Universal Plug and Play (UPnP) -** a set of protocols that allows devices such as gaming consoles, printers, and IoTs on a LAN to detect and connect automatically.
    - UDP 1900 is a popular port used for connection by these devices.

Project

Creating a single payload



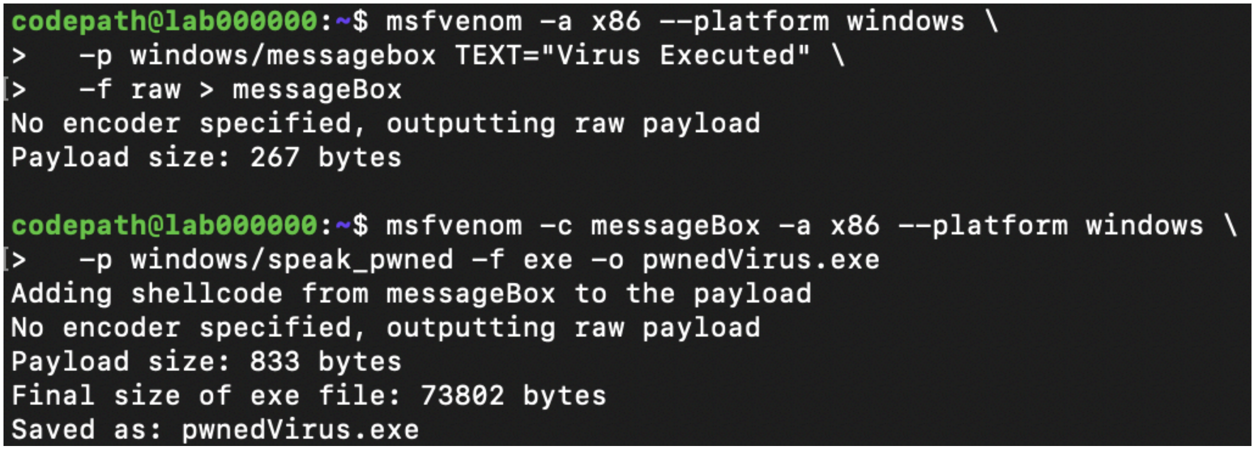
```
codepath@lab000000:~$ msfvenom -a x86 --platform windows -p windows/messagebox TEXT="Virus Executed" -f exe -o messageVirus
.exe

No encoder specified, outputting raw payload
Payload size: 267 bytes
Final size of exe file: 73802 bytes
Saved as: messageVirus.exe
```

Syntax: `msfvenom -a ARCHITECTURE --platform PLATFORM -p PAYLOAD [ARGS] -f FORMAT -o OUTPUTFILE`

- `-a` specifies the computer architecture for the payload.
- `--platform` specifies the OS/programming language the payload will run on.
- `-p` details the functions of the virus (this is the payload).
- `-f` the format of the file.
- `-o` the name of the virus file.

Creating a multi-payload

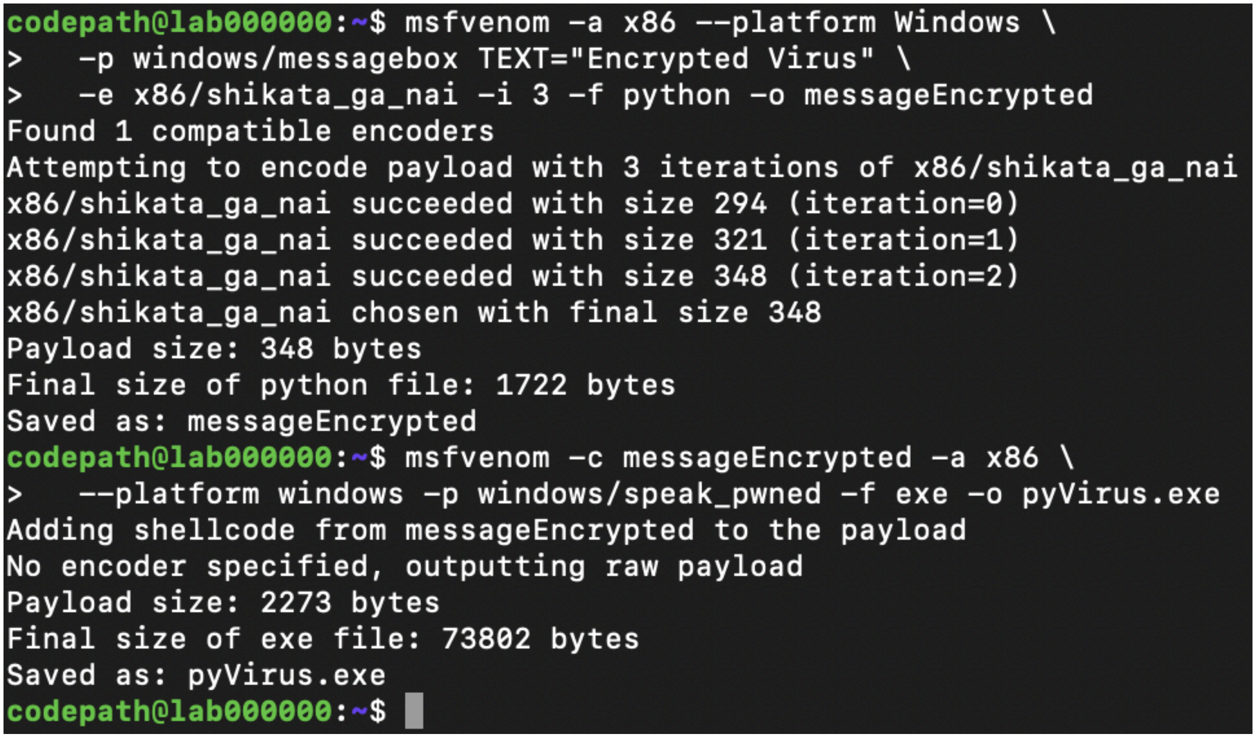


```
codepath@lab000000:~$ msfvenom -a x86 --platform windows \
>   -p windows/messagebox TEXT="Virus Executed" \
[>   -f raw > messageBox
No encoder specified, outputting raw payload
Payload size: 267 bytes

codepath@lab000000:~$ msfvenom -c messageBox -a x86 --platform windows \
[>   -p windows/speak_pwned -f exe -o pwnedVirus.exe
Adding shellcode from messageBox to the payload
No encoder specified, outputting raw payload
Payload size: 833 bytes
Final size of exe file: 73802 bytes
Saved as: pwnedVirus.exe
```

- Create the first payload to create a multi-payload. The `-c` flag allows you to add more payloads. This virus causes the computer to say, "You've been pwned!" aloud.

Creating an encrypted payload



```
codepath@lab000000:~$ msfvenom -a x86 --platform Windows \
>   -p windows/messagebox TEXT="Encrypted Virus" \
>   -e x86/shikata_ga_nai -i 3 -f python -o messageEncrypted
Found 1 compatible encoders
Attempting to encode payload with 3 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 294 (iteration=0)
x86/shikata_ga_nai succeeded with size 321 (iteration=1)
x86/shikata_ga_nai succeeded with size 348 (iteration=2)
x86/shikata_ga_nai chosen with final size 348
Payload size: 348 bytes
Final size of python file: 1722 bytes
Saved as: messageEncrypted
codepath@lab000000:~$ msfvenom -c messageEncrypted -a x86 \
>   --platform windows -p windows/speak_pwned -f exe -o pyVirus.exe
Adding shellcode from messageEncrypted to the payload
No encoder specified, outputting raw payload
Payload size: 2273 bytes
Final size of exe file: 73802 bytes
Saved as: pyVirus.exe
codepath@lab000000:~$
```

- **`x86/shikata_ga_nai`** is a polymorphic XOR additive feedback encoder.