POLITECHNIKA WROCŁAWSKA Wydział Informatyki i Telekomunikacji	Wydział: Informatyki i Telekomunikacji Kierunek: Cyberbezpieczeństwo Rok Akademicki: 2024/2025 Rok studiów, semestr: 2, 4 Grupa: 1 Termin: pon., 7:30

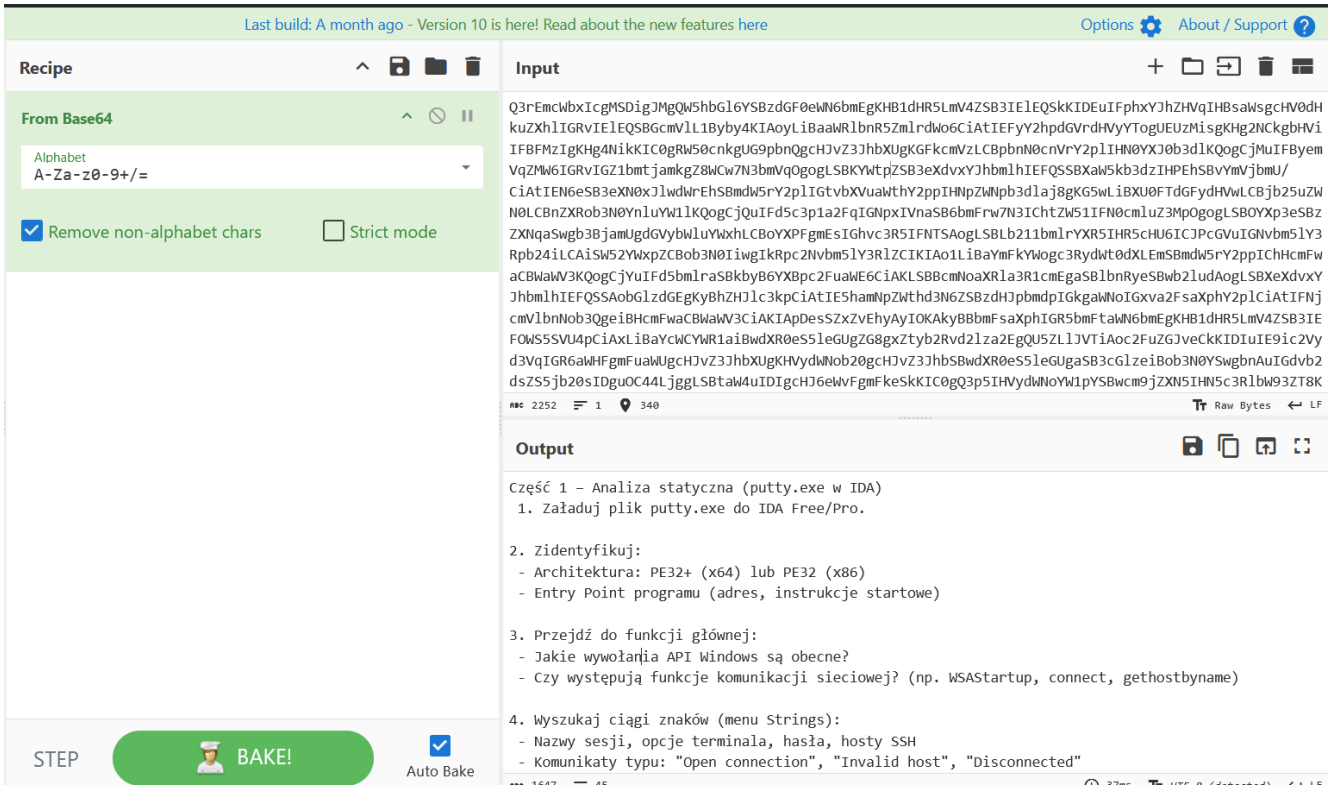
CBESI0053G Informatyka śledcza – Laboratorium 13

Prowadzący: mgr inż. Adrian Florek	Autor: 1. Gerard Błaszczyk
Data wykonania ćwiczenia: 02.06.2025	
Data oddania sprawozdania: 15.06.2025	

1. Cel ćwiczenia

Analiza statyczna i dynamiczna (IDA/ ANY.RUN)

2. Rozszyfrowanie instrukcji laboratoryjnej

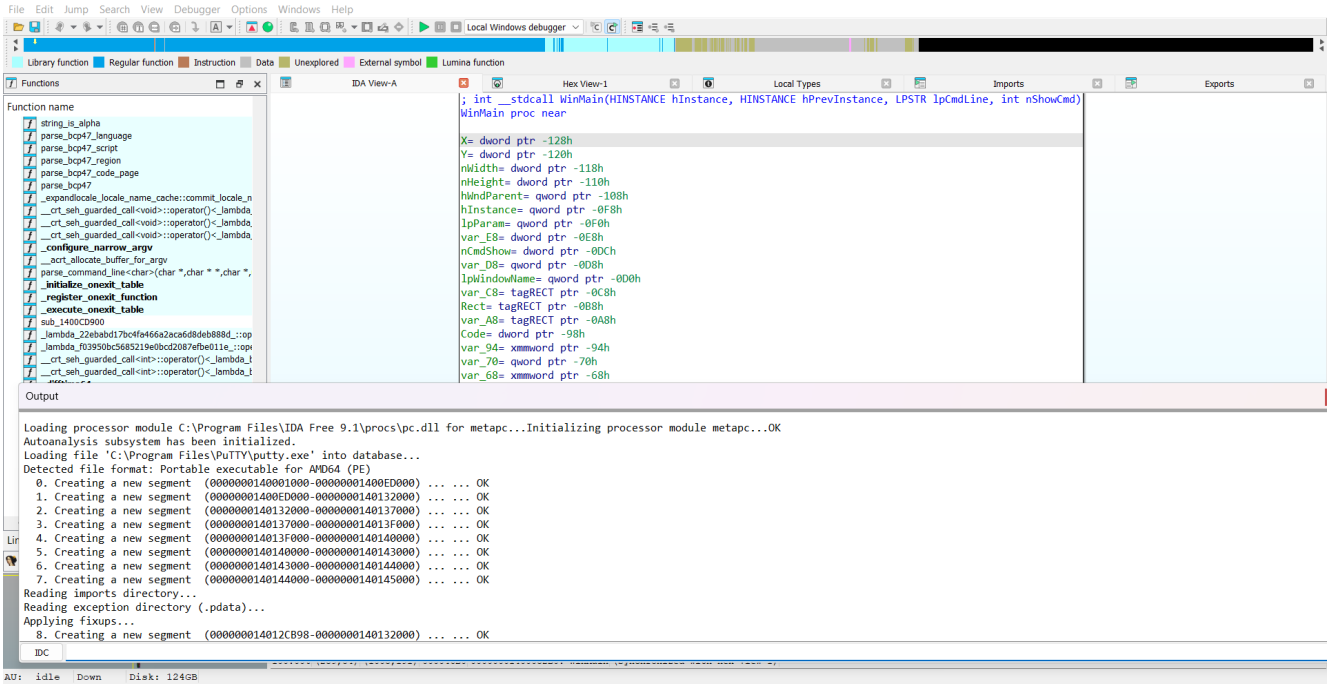


Rysunek 1: CyberChef

3. Realizacja zadań

Część 1 – Analiza statyczna (putty.exe w IDA)

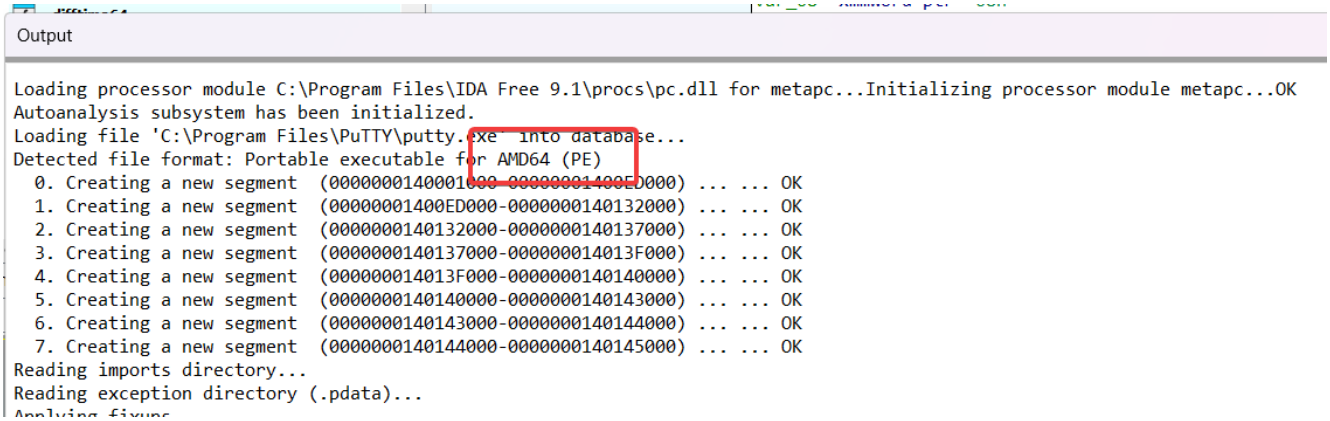
1. Załaduj plik putty.exe do IDA Free/Pro.



Rysunek 2: putty.exe załadowany do IDA

2. Zidentyfikuj:

- Architektura: PE32+ (x64) lub PE32 (x86)



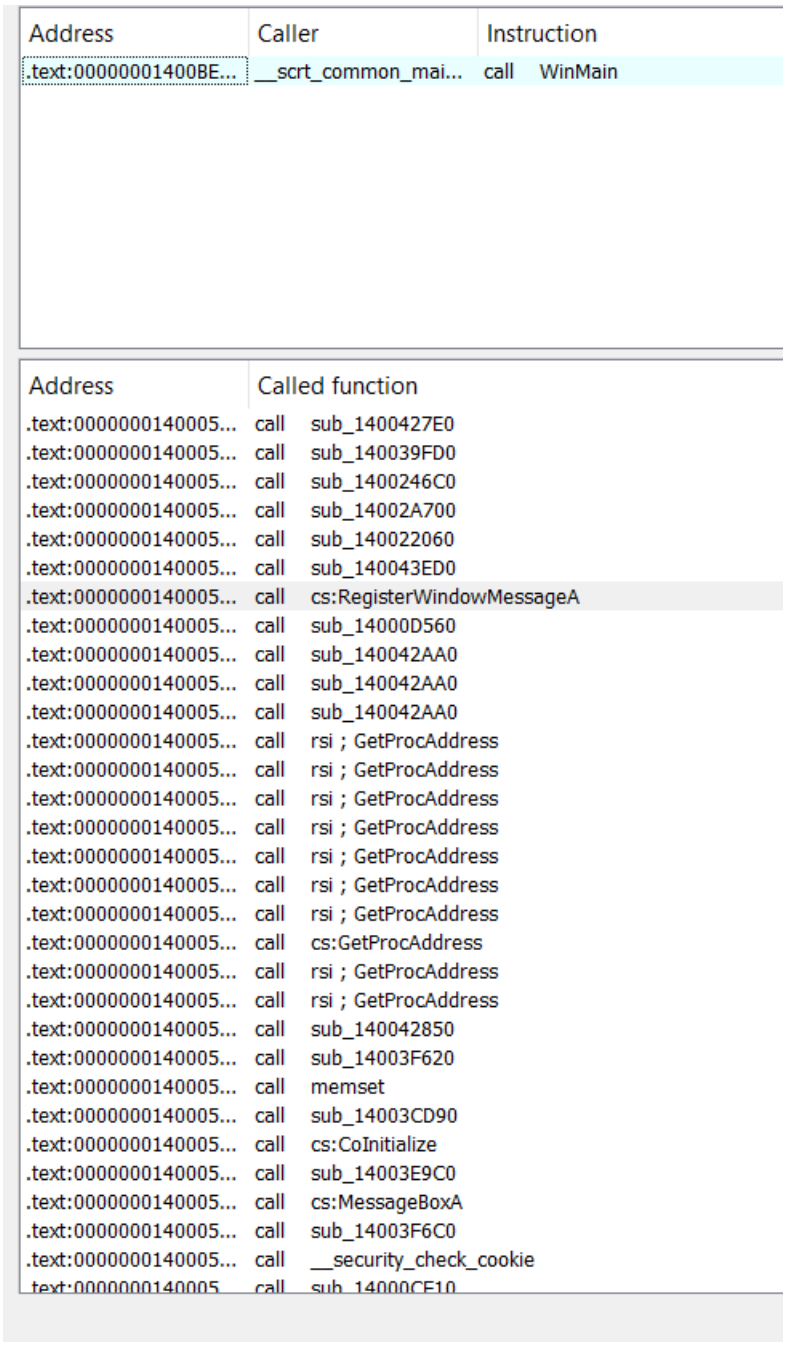
Rysunek 3: Architektura: PE32+ (x64)

- Entry Point programu (adres, instrukcje startowe)

```
.text:0000000140001000 ; __int64 __fastcall sub_140001000(char *Buffer, char *Format)
.text:0000000140001000 sub_140001000   proc near               ; CODE XREF: sub_140008900+A5A↓p
.text:0000000140001000                                         ; sub_140008900+A7E↓p ...
.text:0000000140001000
.text:0000000140001000 Locale          = qword ptr -38h
.text:0000000140001000 ArgList         = qword ptr -30h
.text:0000000140001000 var_28          = qword ptr -28h
.text:0000000140001000 var_20          = qword ptr -20h
.text:0000000140001000 arg_10          = byte ptr  18h
.text:0000000140001000 arg_18          = qword ptr  20h
.text:0000000140001000
.text:0000000140001000                 push    rsi
.text:0000000140001001                 push    rdi
.text:0000000140001002                 push    rbx
.text:0000000140001003                 sub     rsp, 40h
.text:0000000140001007                 mov     rsi, rdx
.text:000000014000100A                 mov     rdi, rcx
.text:000000014000100D                 mov     qword ptr [rsp+58h+arg_10], r8
.text:0000000140001012                 mov     [rsp+58h+arg_18], r9
.text:0000000140001017                 mov     rax, cs:__security_cookie
.text:000000014000101E                 xor     rax, rsp
.text:0000000140001021                 mov     [rsp+58h+var_20], rax
.text:0000000140001026                 lea     rbx, [rsp+58h+arg_10]
.text:000000014000102B                 mov     [rsp+58h+var_28], rbx
.text:0000000140001030                 call    sub_140007520
.text:0000000140001035                 mov     rcx, [rax]
.text:0000000140001038                 or      rcx, 1          ; Options
.text:000000014000103C                 mov     [rsp+58h+ArgList], rbx ; ArgList
.text:0000000140001041                 mov     [rsp+58h+Locale], 0 ; Locale
.text:000000014000104A                 mov     rdx, rdi        ; Buffer
.text:000000014000104D                 mov     r8, 0FFFFFFFFFFFFFFFFh ; BufferCount
```

Rysunek 4: początkowe instrukcje i adresy

3. Przejdź do funkcji głównej:
- Jakie wywołania API Windows są obecne?
- Czy występują funkcje komunikacji sieciowej? (np. WSAStartup, connect, gethostbyname)

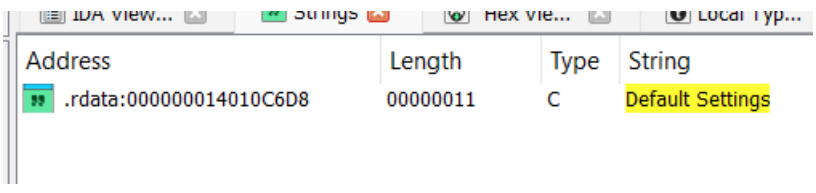


Rysunek 5: sekcja „function calls” dla funkcji „WinMain”

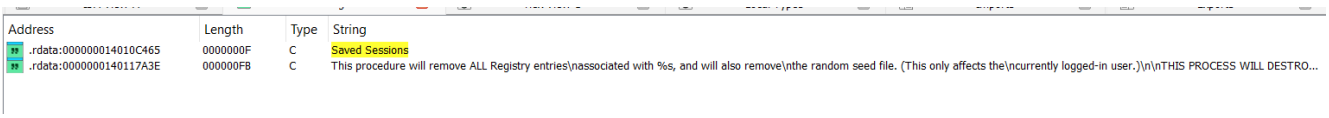
Odp: występują odwołania do API Windows np. RegisterWindowMessageA, GetProcAddress, CoInitialize

W wywołanych przez funkcję *WinMain* funkcjach nie odnalazłem funkcji komunikacji sieciowej.

4. Wyszukaj ciągi znaków (menu Strings):
- Nazwy sesji, opcje terminala, hasła, hosty SSH
- Komunikaty typu: "Open connection", "Invalid host", "Disconnected"



Rysunek 6: znalezione ciągi

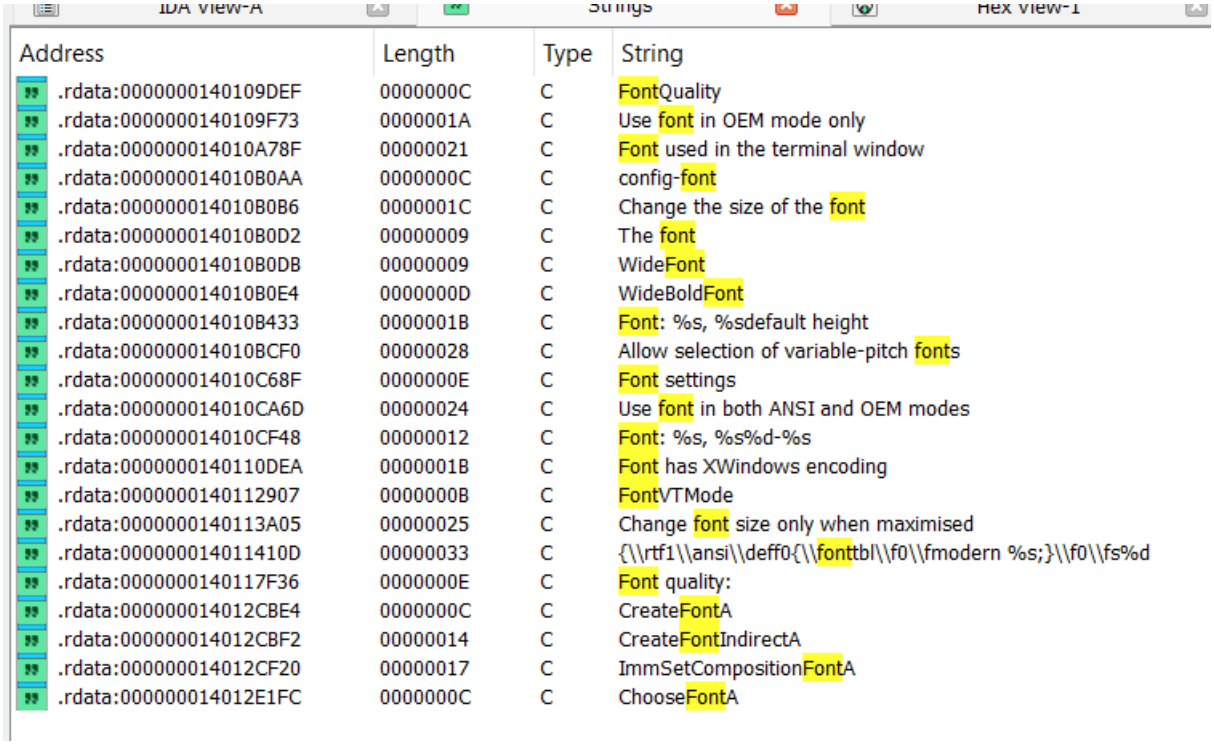


Address	Length	Type	String
.rdata:000000014010C465	0000000F	C	Saved Sessions
.rdata:000000140117A3E	000000FB	C	This procedure will remove ALL Registry entries\nassociated with %s, and will also remove\nthe random seed file. (This only affects the\ncurrently logged-in user.)\n\nTHIS PROCESS WILL DESTRO...

Rysunek 7: znalezione ciągi

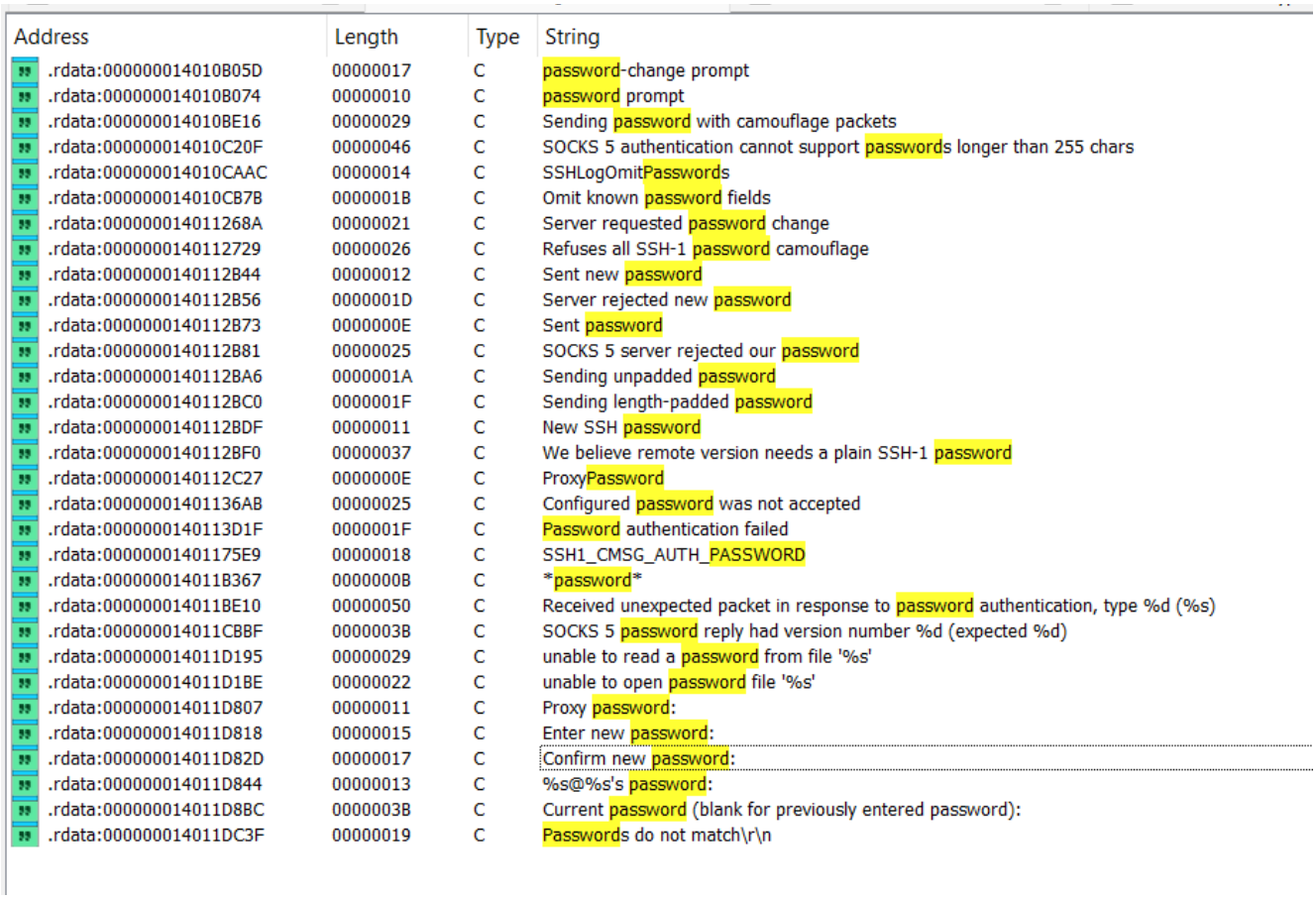
Address	Length	Type	String
.rdata:0000000140109E97	00000016	C	Window/Selection/Copy
.rdata:000000014010A600	0000000E	C	FlashWindowEx
.rdata:000000014010A6C8	00000020	C	Options controlling %s's window
.rdata:000000014010A6E8	00000027	C	Configure the behaviour of %s's window
.rdata:000000014010A70F	00000028	C	Configure the appearance of %s's window
.rdata:000000014010A737	00000029	C	Hide mouse pointer when typing in window
.rdata:000000014010A760	0000002F	C	Print proxy diagnostics in the terminal window
.rdata:000000014010A78F	00000021	C	Font used in the terminal window
.rdata:000000014010A7B0	0000001B	C	Warn before closing window
.rdata:000000014010A7CB	0000001C	C	PuTTY: hidden timing window
.rdata:000000014010A7E7	00000025	C	Control the scrollback in the window
.rdata:000000014010A80C	0000001B	C	Set the size of the window
.rdata:000000014010A827	00000011	C	PuTTYTimerWindow
.rdata:000000014010A838	00000012	C	MonitorFromWindow
.rdata:000000014010BB72	0000000C	C	x86 Windows
.rdata:000000014010BFD2	0000000C	C	WindowClass
.rdata:000000014010C07E	0000000F	C	Window/Colours
.rdata:000000014010C931	00000020	C	Separate window and icon titles
.rdata:000000014010D409	00000025	C	Unable to create terminal window: %s
.rdata:000000014010DA77	00000012	C	GetDC(window): %s
.rdata:000000014010DA89	0000002A	C	CreateCompatibleDC(desktop window dc): %s
.rdata:000000014010DCD0	00000011	C	Window/Behaviour
.rdata:000000014010E1DD	00000019	C	Adjust the window border
.rdata:000000014010E1F6	0000000D	C	WindowBorder
.rdata:000000014010E458	0000001F	C	Ensure window is always on top
.rdata:000000014010EA65	00000011	C	Window/Selection
.rdata:000000014010EBA2	00000013	C	Window/Translation
.rdata:000000014010FF5A	00000036	C	window adjustment after downstream accepted X channel
.rdata:00000001401102CB	00000019	C	AdjustWindowRectExForDpi
.rdata:0000000140110C33	00000030	C	Disable remote-controlled window title changing
.rdata:0000000140110DEA	0000001B	C	Font has XWindows encoding
.rdata:0000000140111446	00000016	C	DwmGetWindowAttribute
.rdata:0000000140111D8A	00000029	C	Adjust the behaviour of the window title
.rdata:0000000140111DB3	0000000D	C	Window title
.rdata:000000014011267C	0000000E	C	window-change
.rdata:00000001401129AB	00000012	C	Window/Appearance
.rdata:0000000140114BAD	0000001F	C	SSH2_MSG_CHANNEL_WINDOW_ADJUST
.rdata:00000001401170C6	00000016	C	SSH1_CMSG_WINDOW_SIZE
.rdata:00000001401180FB	00000016	C	Close window on exit:
.rdata:00000001401185F2	0000000E	C	Window title:
.rdata:0000000140118600	00000022	C	Gap between text and window edge:
.rdata:00000001401186B0	00000018	C	When window is resized:

Rysunek 8: znalezione ciągi



Address	Length	Type	String
.rdata:0000000140109DEF	0000000C	C	FontQuality
.rdata:0000000140109F73	0000001A	C	Use font in OEM mode only
.rdata:000000014010A78F	00000021	C	Font used in the terminal window
.rdata:000000014010B0AA	0000000C	C	config-font
.rdata:000000014010B0B6	0000001C	C	Change the size of the font
.rdata:000000014010B0D2	00000009	C	The font
.rdata:000000014010B0DB	00000009	C	WideFont
.rdata:000000014010B0E4	0000000D	C	WideBoldFont
.rdata:000000014010B433	0000001B	C	Font: %s, %sdefault height
.rdata:000000014010BCF0	00000028	C	Allow selection of variable-pitch fonts
.rdata:000000014010C68F	0000000E	C	Font settings
.rdata:000000014010CA6D	00000024	C	Use font in both ANSI and OEM modes
.rdata:000000014010CF48	00000012	C	Font: %s, %s%d-%s
.rdata:0000000140110DEA	0000001B	C	Font has XWindows encoding
.rdata:0000000140112907	0000000B	C	FontVTMode
.rdata:0000000140113A05	00000025	C	Change font size only when maximised
.rdata:000000014011410D	00000033	C	{\\rtf1\\ansi\\deff0{\\fonttbl\\f0\\fmodern %s;}\\f0\\fs%d
.rdata:0000000140117F36	0000000E	C	Font quality:
.rdata:000000014012CBE4	0000000C	C	CreateFontA
.rdata:000000014012CBF2	00000014	C	CreateFontIndirectA
.rdata:000000014012CF20	00000017	C	ImmSetCompositionFontA
.rdata:000000014012E1FC	0000000C	C	ChooseFontA

Rysunek 9: znalezione ciągi

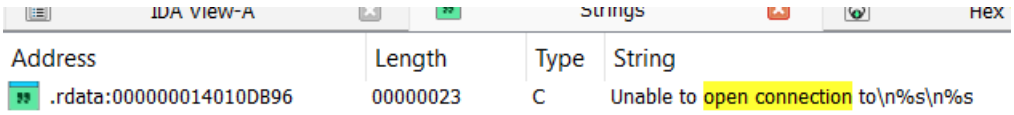


Address	Length	Type	String
.rdata:000000014010B05D	00000017	C	password-change prompt
.rdata:000000014010B074	00000010	C	password prompt
.rdata:000000014010BE16	00000029	C	Sending password with camouflage packets
.rdata:000000014010C20F	00000046	C	SOCKS 5 authentication cannot support passwords longer than 255 chars
.rdata:000000014010CAAC	00000014	C	SSHLogOmitPasswords
.rdata:000000014010CB7B	0000001B	C	Omit known password fields
.rdata:000000014011268A	00000021	C	Server requested password change
.rdata:0000000140112729	00000026	C	Refuses all SSH-1 password camouflage
.rdata:0000000140112B44	00000012	C	Sent new password
.rdata:0000000140112B56	0000001D	C	Server rejected new password
.rdata:0000000140112B73	0000000E	C	Sent password
.rdata:0000000140112B81	00000025	C	SOCKS 5 server rejected our password
.rdata:0000000140112BA6	0000001A	C	Sending unpadded password
.rdata:0000000140112BC0	0000001F	C	Sending length-padded password
.rdata:0000000140112BDF	00000011	C	New SSH password
.rdata:0000000140112BF0	00000037	C	We believe remote version needs a plain SSH-1 password
.rdata:0000000140112C27	0000000E	C	ProxyPassword
.rdata:00000001401136AB	00000025	C	Configured password was not accepted
.rdata:0000000140113D1F	0000001F	C	Password authentication failed
.rdata:00000001401175E9	00000018	C	SSH1_CMSG_AUTH_PASSWORD
.rdata:000000014011B367	0000000B	C	*password*
.rdata:000000014011BE10	00000050	C	Received unexpected packet in response to password authentication, type %d (%s)
.rdata:000000014011CBBF	0000003B	C	SOCKS 5 password reply had version number %d (expected %d)
.rdata:000000014011D195	00000029	C	unable to read a password from file '%s'
.rdata:000000014011D1BE	00000022	C	unable to open password file '%s'
.rdata:000000014011D807	00000011	C	Proxy password:
.rdata:000000014011D818	00000015	C	Enter new password:
.rdata:000000014011D82D	00000017	C	Confirm new password:
.rdata:000000014011D844	00000013	C	%s@%s's password:
.rdata:000000014011D8BC	0000003B	C	Current password (blank for previously entered password):
.rdata:000000014011DC3F	00000019	C	Passwords do not match\r\n

Rysunek 10: znalezione ciągi

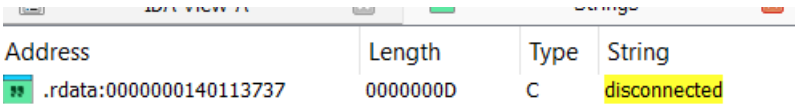
Address	Length	Type	String
.rdata:00000001400F3130	0000015C	C	You are loading an SSH-2 private key which has an\nold version of the file format. This means your key\nfile is not fully tamperproof. Future versions of\n%s may stop supporting this private key ...
.rdata:00000001400F8890	0000002F	C	SSHCONNECTION@putty.projects.tartarus.org-2.0-
.rdata:0000000140109CCD	00000007	C	sshtty
.rdata:0000000140109CDF	0000000F	C	config-ssh-pty
.rdata:0000000140109D49	00000016	C	config-ssh-xauthority
.rdata:0000000140109FFE	00000022	C	config-ssh-portfwd-address-family
.rdata:000000014010A088	00000024	C	Handles SSH-2 key re-exchange badly
.rdata:000000014010A0DE	00000013	C	config-ssh-privkey
.rdata:000000014010A10B	00000015	C	config-ssh-kex-rekey
.rdata:000000014010A120	00000015	C	config-ssh-bug-rekey
.rdata:000000014010A1B0	00000031	C	Noninteractive SSH proxy cannot confirm host key
.rdata:000000014010A1E1	0000003D	C	Noninteractive SSH proxy cannot confirm weak cached host key
.rdata:000000014010A292	0000001A	C	ssh.com SSH-2 private key
.rdata:000000014010A2AC	0000001E	C	not a PuTTY SSH-2 private key
.rdata:000000014010A2CA	0000002E	C	not a public key or a PuTTY SSH-2 private key
.rdata:000000014010A2F8	00000012	C	SSH-1 private key
.rdata:000000014010A399	00000011	C	SSH-1 public key
.rdata:000000014010A5C8	00000013	C	Connection/SSH/Kex
.rdata:000000014010ACA1	0000001D	C	config-ssh-portfwd-localhost
.rdata:000000014010AFB5	00000014	C	config-ssh-kex-cert
.rdata:000000014010AFC9	00000010	C	config-ssh-cert
.rdata:000000014010AFDF	00000019	C	config-ssh-bug-dropstart
.rdata:000000014010B092	00000010	C	config-ssh-prot
.rdata:000000014010B0A2	00000008	C	SshProt
.rdata:000000014010B26D	00000014	C	config-ssh-tryagent
.rdata:000000014010B399	0000001E	C	config-ssh-bug-filter-kexinit
.rdata:000000014010B675	0000001C	C	Bad SSH-1 public key packet
.rdata:000000014010B91D	00000021	C	config-ssh-prefer-known-hostkeys
.rdata:000000014010B93E	0000001F	C	config-ssh-kex-manual-hostkeys
.rdata:000000014010B997	00000022	C	Options controlling SSH host keys
.rdata:000000014010B9B9	00000019	C	Connection/SSH/Host keys
.rdata:000000014010B9D2	00000022	C	Miscomputes SSH-2 encryption keys
.rdata:000000014010BA47	0000001C	C	Miscomputes SSH-2 HMAC keys
.rdata:000000014010BA63	0000001B	C	Pageant has %zu SSH-2 keys
.rdata:000000014010BA7E	0000001B	C	Pageant has %zu SSH-1 keys
.rdata:000000014010BABE	00000012	C	SSHManualHostKeys
.rdata:000000014010BAD0	00000027	C	Software\\SimonTatham\\PuTTY\\SshHostKeys
.rdata:000000014010BC48	0000002A	C	Chokes on PuTTY's SSH-2 'winadj' requests
.rdata:000000014010BE3F	0000000C	C	SSH packets
.rdata:000000014010BF7C	00000014	C	opensshcert-ssh-dss
.rdata:000000014010C0A2	00000027	C	Detection of known bugs in SSH servers
.rdata:000000014010C3E2	00000024	C	Options controlling SSH connections

Rysunek 11: znalezione ciągi



Address	Length	Type	String
.rdata:000000014010DB96	00000023	C	Unable to open connection to\n%s\n%s

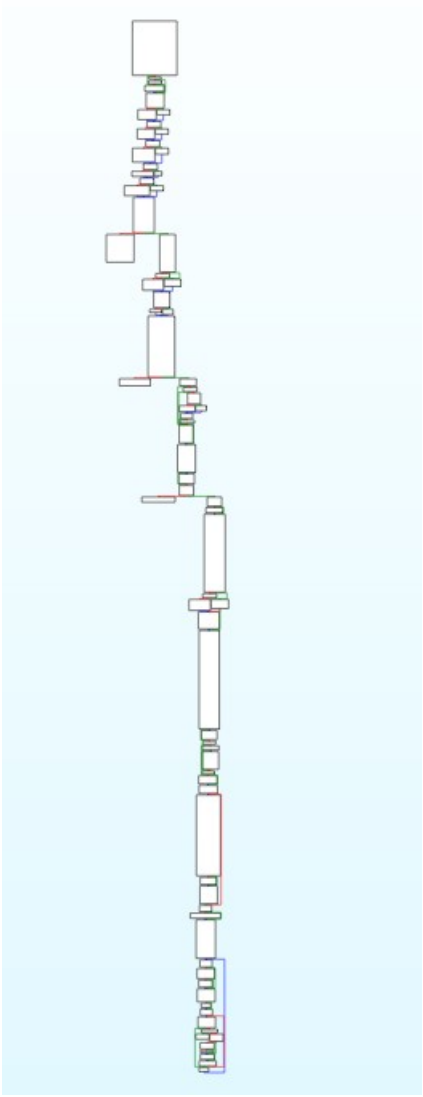
Rysunek 12: znalezione ciągi



Address	Length	Type	String
.rdata:0000000140113737	0000000D	C	disconnected

Rysunek 13: znalezione ciągi

5. Zbadaj strukturę funkcji (Graph View)



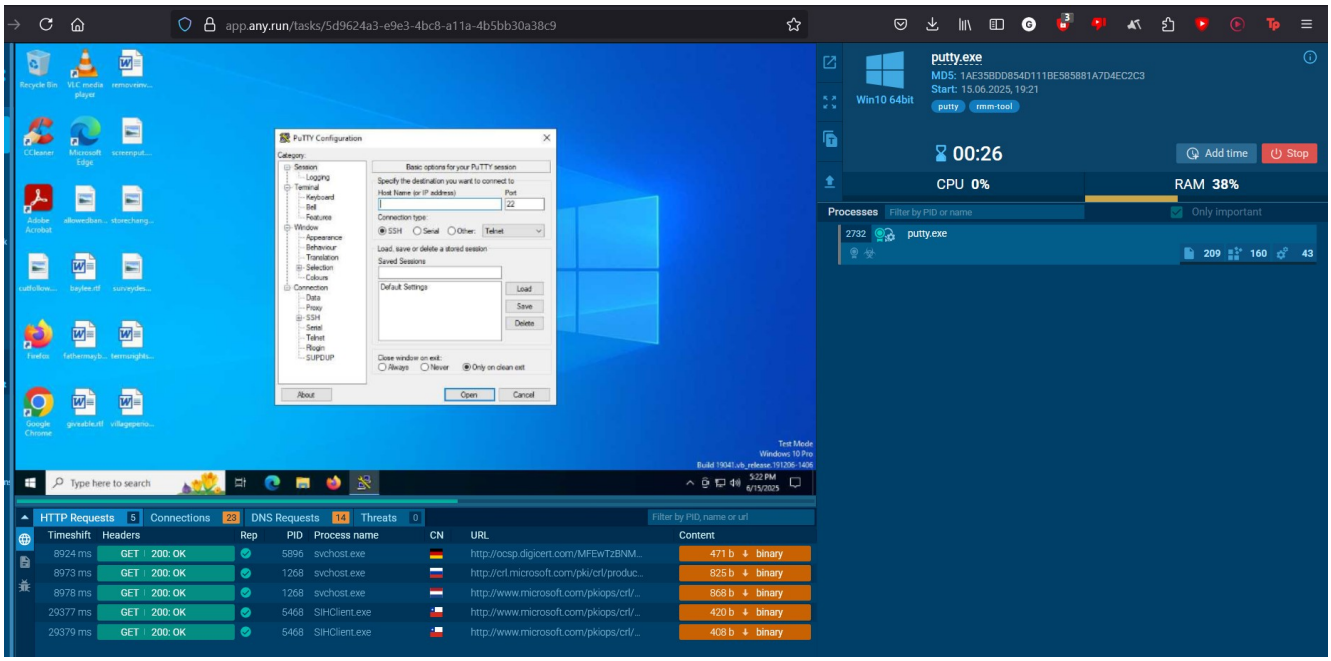
Rysunek 14: Struktura funkcji

Wnioski dot. struktury:

- Graf ma wyraźnie liniową strukturę z dużą liczbą następujących po sobie bloków.
- Nie ma skomplikowanych, głęboko zagnieżdżonych struktur, ani dużej liczby równoległych ścieżek.
- Na dolnej części grafu widać pętle.

Część 2 – Analiza dynamiczna (putty.exe w ANY.RUN)

1. Załaduj putty.exe do środowiska ANY.RUN (sandbox)

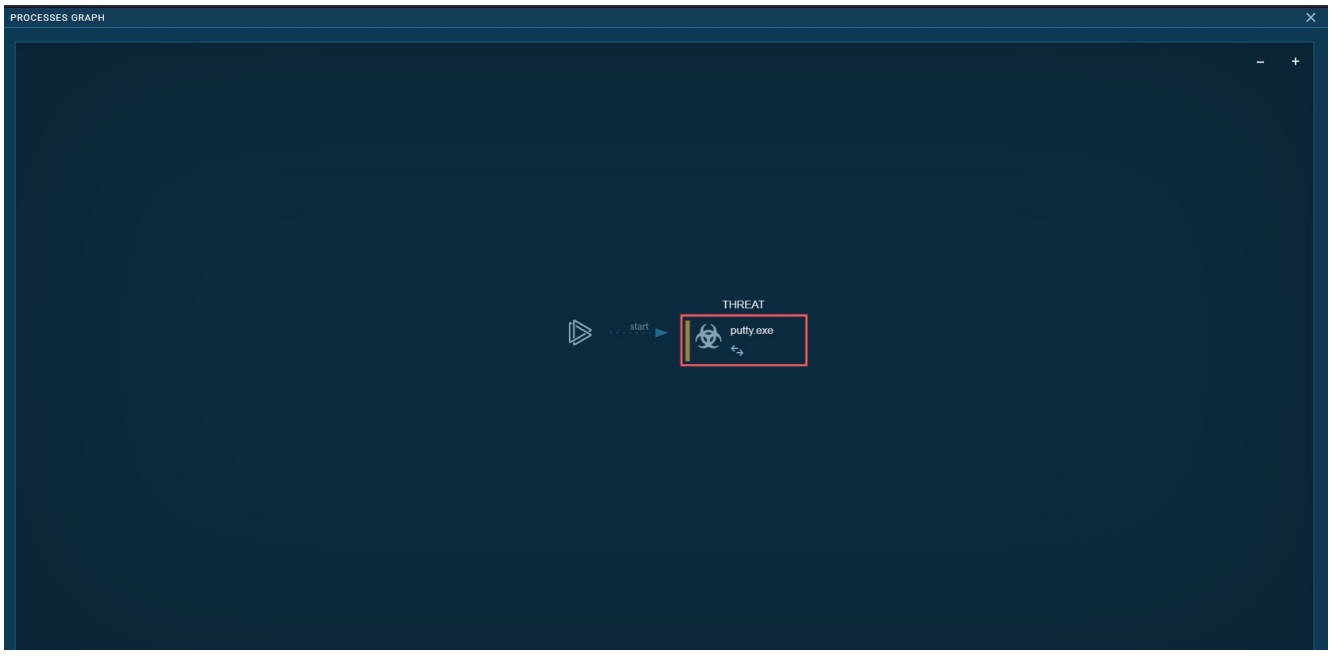


Rysunek 15: ANY.RUN

2. Obserwuj działanie programu (uruchom program putty.exe i wpisz hosta, np. google.com, 8.8.8.8 - min. 2 przykłady)
- Czy uruchamia procesy systemowe?
- Czy łączy się z adresem IP lub domeną po wpisaniu hosta?
- Czy odczytuje/zapisuje pliki konfiguracyjne?

Przykład 1: adres – 8.8.8.8

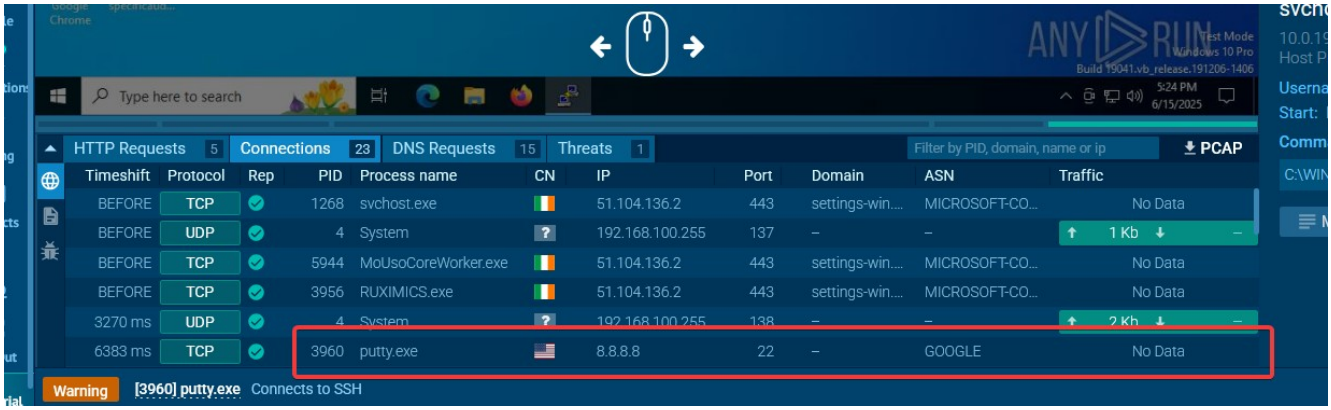
- Czy uruchamia procesy systemowe?



Rysunek 16: uruchamiane procesy podczas testu

Nie – program nie uruchomił procesów systemowych

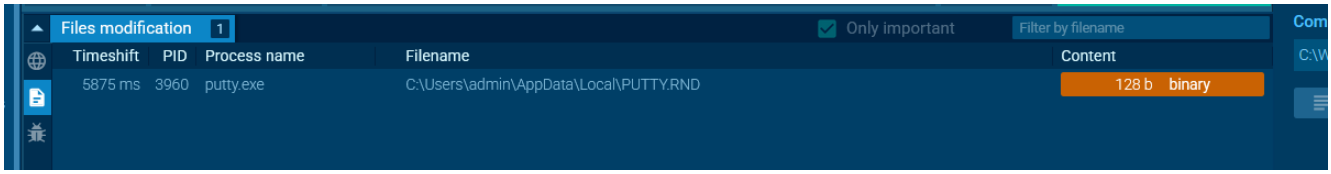
- Czy łączy się z adresem IP lub domeną po wpisaniu hosta?



Rysunek 17: połączenia podczas testu

Tak, program łączy się z adresem 8.8.8.8

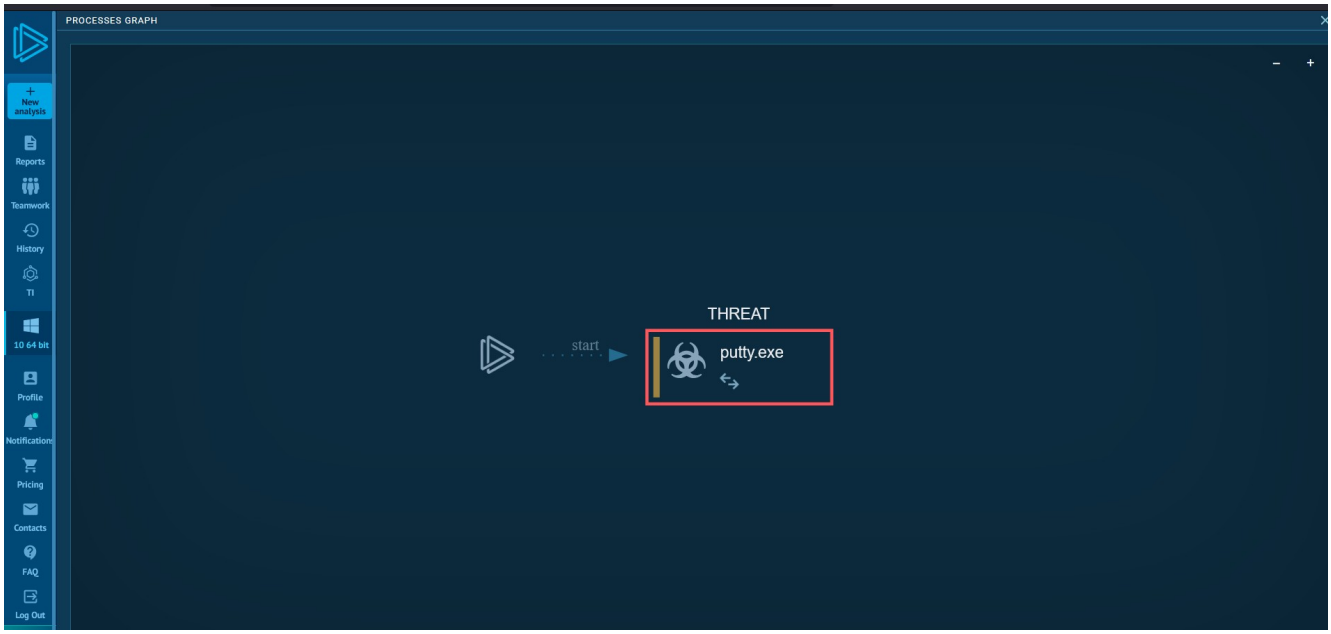
- Czy odczytuje/zapisuje pliki konfiguracyjne?



Rysunek 18: zmienione pliki podczas testu

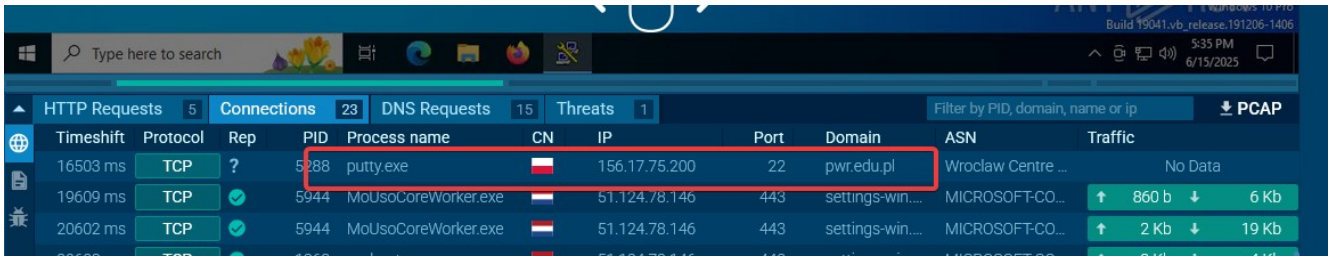
Tak, program zmienia plik PUTTY.RND

Przykład 2. adres – pwr.edu.pl



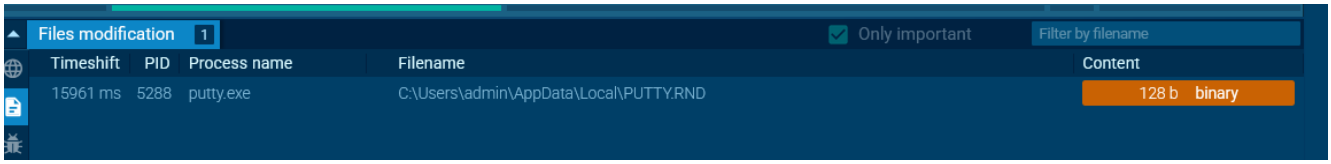
Rysunek 19: uruchamiane procesy podczas testu

Nie – program nie uruchomił procesów systemowych



Rysunek 20: połączenia podczas testu

Tak, program łączy się z adresem pwr.edu.pl

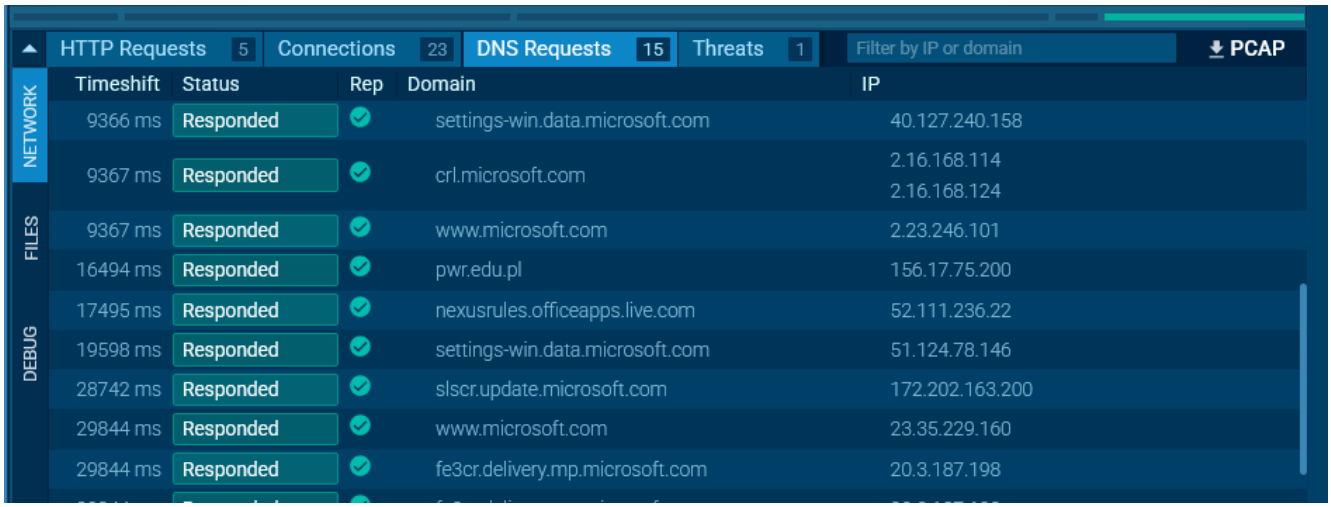


Rysunek 21: uruchamiane procesy podczas testu

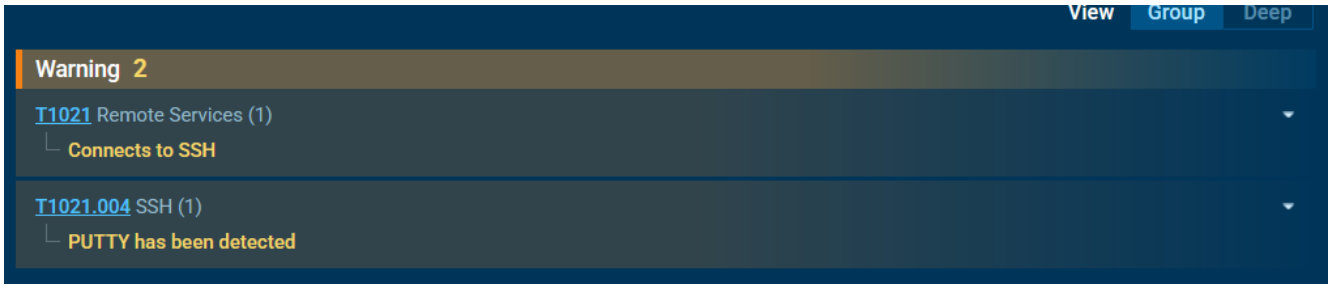
Tak, program zmienia plik PUTTY.RND

3. Zidentyfikuj:
- Tworzenie plików (np. putty.ini, sesje)
- Ruch sieciowy (domeny, adresy IP, porty)
- Zmiany w rejestrze

Fragmenty potrzebne do zadania 3. zostały przedstawione w odpowiedzi na zadanie 2.
Inne aspekty analizy:



Rysunek 22: zapytania DNS



Rysunek 23: zagrożenia wg ANY.RUN

4. Wnioski

Zarówno analiza statyczna jak i dynamiczna dostarczają ważnych informacji w kontekście informatyki śledczej.