



# Windbgshark:

the unified traffic instrumentation tool <sup>[1,2,3]</sup>

1. Virtualized
2. For Windows
3. For vulnerability researchers and reverse engineers

Labunets Andrey

**ZERO NIGHTS** 25.11.11

# Preamble

There are so many fuzzers, frameworks, code debuggers, etc.

Give me a simple network debugging tool under windows instead.

Why?

# I tried physical MITM

\* ...or virtual

+ obvious

– no localhost traffic

# I tried user-mode magic

- \* code debuggers
  - \* hooks, binary instrumentation
  - \* LSP
- 
- + stack backtraces available
  - + ssl decryption is possible (ospy)
- 
- not handy for traffic manipulation
  - x64?
  - layer < 7? non-winsock? (ICMP, SMB, ...)

# I tried handling network interfaces

- \* NDIS

- + one driver for all traffic

- no localhost traffic

- need to reconstruct TCP/IP stack

# I tried some kernel-mode magic

- \* Windows Filtering Platform

- + unified

- + multi-level (OSI)

- only starting from Vista

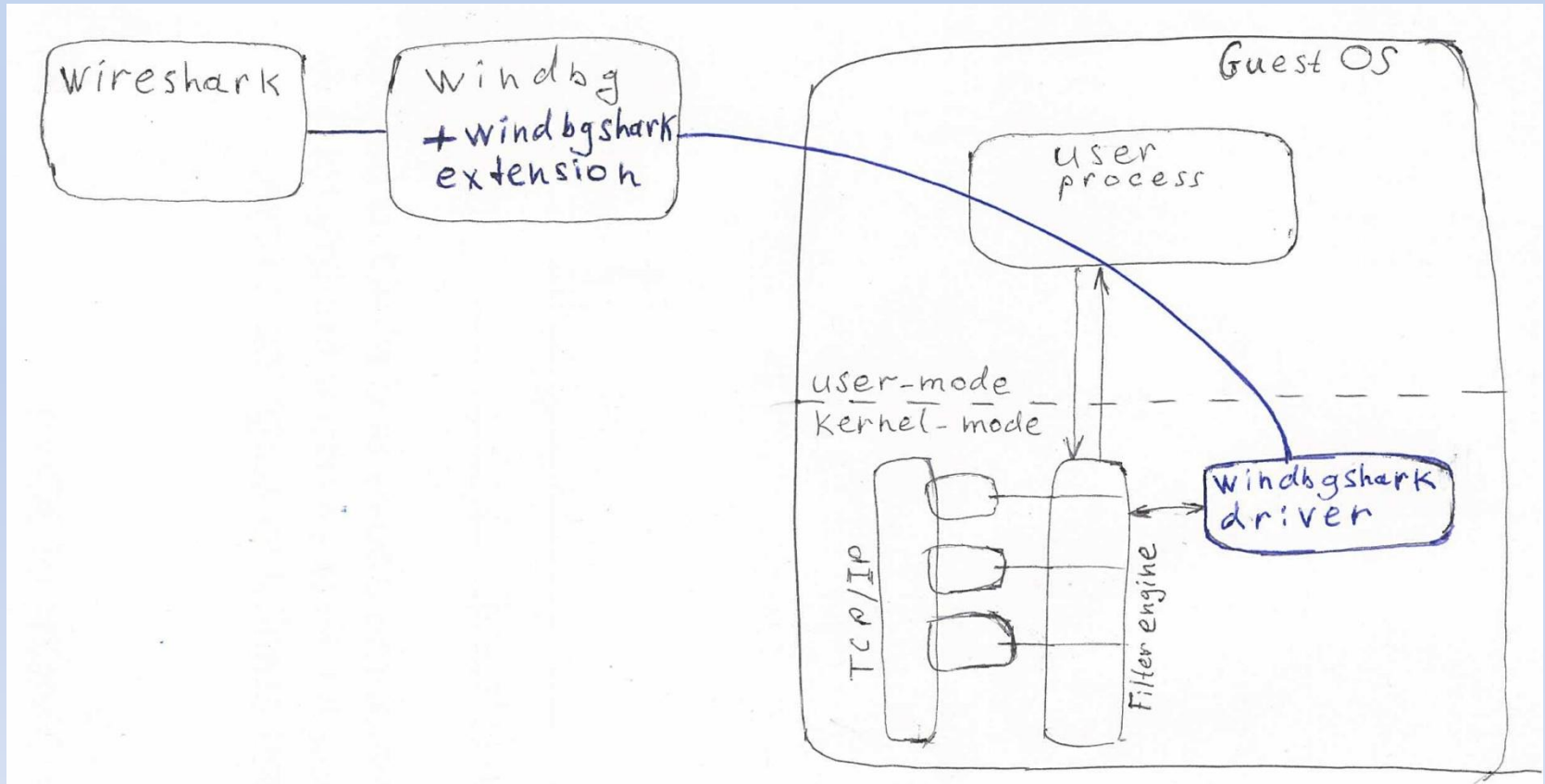
- (reasonable trade-off, TDI on WinXP is almost the same)

# We developed windbgshark

...VM-based traffic manipulation tool

- \* wfp driver as a mechanism (guest OS)
- \* windbg extension as a control interface (host OS)
- \* wireshark for packet analysis (host OS)

# Theory of operation





# Quickstart

```
> !load windbgshark
```

```
> !strace on
```

```
> g
```

```
...
```

```
> !packet 100 +AAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
[look in wireshark]
```

```
> g
```

```
...
```

# Quickstart

Command - Kernel 'com:pipe, resets=0, reconnect, port=\\.\pipe\kd\_Windows\_7\_x64\_La

```

db FFFFF8001063010 L156
fffffa80`01063010 48 54 54 50 2f 31 2e 31-20 33 30 32 20 4d 6f 76 HTTP/1.1 302 Mov
fffffa80`01063020 65 64 20 54 65 6d 70 6f-72 61 72 69 6c 79 0d 0a ed Temporarily..
fffffa80`01063030 53 65 72 76 65 72 3a 20-6e 67 69 6e 78 0d 0a 44 Server: nginx..D
fffffa80`01063040 61 74 65 3a 20 57 65 64-2c 20 32 33 20 4e 6f 76 ate: Wed, 23 Nov
fffffa80`01063050 20 32 30 31 31 20 31 39-3a 33 39 3a 31 33 20 47 2011 19:39:13 G
fffffa80`01063060 4d 54 0d 0a 43 6f 6e 74-65 6e 74 2d 54 79 70 65 MT..Content-Type
fffffa80`01063070 3a 20 74 65 78 74 2f 68-74 6d 6c 0d 0a 43 6f 6e : text/html..Con
fffffa80`01063080 74 65 6e 74 2d 4c 65 6e-67 74 68 3a 20 31 35 34 tent-Length: 154
fffffa80`01063090 0d 0a 43 6f 6e 6e 65 63-74 69 6f 6e 3a 20 63 6c ..Connection: cl
fffffa80`010630a0 6f 73 65 0d 0a 4c 6f 63-61 74 69 6f 6e 3a 20 68 0e ose..Location: h
fffffa80`010630b0 74 74 70 3a 2f 2f 79 61-6e 64 65 78 2e 72 75 2f ttp://yandex.ru/
fffffa80`010630c0 34 30 34 2e 68 74 6d 6c-0d 0a 0d 0a 3c 68 74 6d 404.html...<htm
fffffa80`010630d0 6c 3e 0d 0a 3c 68 65 61-64 3e 3c 74 69 74 6c 65 l>..<head><title
fffffa80`010630e0 3e 33 30 32 20 46 6f 75-6e 64 3c 2f 74 69 74 6c >302 Found</titl
fffffa80`010630f0 65 3e 3c 2f 68 65 61 64-3e 0d 0a 3c 62 6f 64 79 e></head>..<body
fffffa80`01063100 20 62 67 63 6f 6c 6f 72-3d 22 77 68 69 74 65 22 bgcolor="white"
fffffa80`01063110 3e 0d 0a 3c 63 65 6e 74-65 72 3e 3c 68 31 3e 33 >..<center><h1>302 Fo
fffffa80`01063120 30 32 20 46 6f 75 6e 64-3c 2f 68 31 3e 3c 2f 02 Found</h1></center>
fffffa80`01063130 65 6e 74 65 72 3e 0d 0a-3c 68 72 3e 3c 63 65 6e enter>..<hr><cen
fffffa80`01063140 74 65 72 3e 6e 67 69 6e-78 3c 2f 63 65 6e 74 65 6e ter>nginx</cente
fffffa80`01063150 72 3e 0d 0a 3c 2f 62 6f-64 79 3e 0d 0a 3c 2f 68 r>..</body>..</h
fffffa80`01063160 74 6d 6c 3e 0d 0a
windbgshark_drv!inspectPacket+0xd4:
fffffa80`035f2874 call windbgshark_drv!nop (fffffa80`035f2d10)
kd> !packet 100 +AAAAAAAAAAAAAAAAAAAAAAAAAAAA
db FFFFF8001063010 L171
fffffa80`01063010 48 54 54 50 2f 31 2e 31-20 33 30 32 20 4d 6f 76 HTTP/1.1 302 Mov
fffffa80`01063020 65 64 20 54 65 6d 70 6f-72 61 72 69 6c 79 0d 0a ed Temporarily..
fffffa80`01063030 53 65 72 76 65 72 3a 20-6e 67 69 6e 78 0d 0a 44 Server: nginx..D
fffffa80`01063040 61 74 65 3a 20 57 65 64-2c 20 32 33 20 4e 6f 76 ate: Wed, 23 Nov
fffffa80`01063050 20 32 30 31 31 20 31 39-3a 33 39 3a 31 33 20 47 2011 19:39:13 G
fffffa80`01063060 4d 54 0d 0a 43 6f 6e 74-65 6e 74 2d 54 79 70 65 MT..Content-Type
fffffa80`01063070 3a 20 74 65 78 74 2f 68-74 6d 6c 0d 0a 43 6f 6e : text/html..Con
fffffa80`01063080 74 65 6e 74 2d 4c 65 6e-67 74 68 3a 20 31 35 34 tent-Length: 154
fffffa80`01063090 0d 0a 43 6f 6e 6e 65 63-74 69 6f 6e 3a 20 63 6c ..Connection: cl
fffffa80`010630a0 6f 73 65 0d 0a 4c 6f 63-61 74 69 6f 6e 3a 20 68 0e ose..Location: h
fffffa80`010630b0 74 74 70 3a 2f 2f 79 61-6e 64 65 78 2e 72 75 2f ttp://yandex.ru/
fffffa80`010630c0 34 30 34 2e 68 74 6d 6c-0d 0a 0d 0a 3c 68 74 6d 404.html...<htm
fffffa80`010630d0 6c 3e 0d 0a 3c 68 65 61-64 3e 3c 74 69 74 6c 65 l>..<head><title
fffffa80`010630e0 3e 33 30 32 20 46 6f 75 6e 64-3c 2f 74 69 74 6c >302 Found</titl
fffffa80`010630f0 65 3e 3c 2f 68 65 61 64-3e 0d 0a 3c 62 6f 64 79 e></head>..<body
fffffa80`01063100 20 62 67 63 6f 6c 6f 72-3d 22 77 68 69 74 65 22 bgcolor="white"
fffffa80`01063110 41 41 41 41 41 41 41 41-41 41 41 41 41 41 41 AAAAAAAAAAAAAAA
fffffa80`01063120 41 41 41 41 41 41 41 41-41 41 41 41 41 41 41 ..<
fffffa80`01063130 65 6e 74 65 72 3e 3c 68-31 3e 33 30 32 20 46 6f enter><h1>302 Fo
fffffa80`01063140 75 6e 64 3c 2f 68 31 3e-3c 2f 63 65 6e 74 65 72 0d 0a 3c 2f 02 Found</h1></center>
fffffa80`01063150 3e 0d 0a 3c 68 72 3e 3c-63 65 6e 74 65 72 3e 3c 6e >..<hr><center>n
fffffa80`01063160 67 69 6e 78 3c 2f 63 65-6e 74 65 72 3e 0d 0a 3c 2f 68 ginx</center>..<
fffffa80`01063170 2f 62 6f 64 79 3e 0d 0a-3c 2f 68 74 6d 6c 3e 0d /body>..</html>.
fffffa80`01063180 0a

```

No.	Time	Source	Destination
61	2011-11-24 00:47:55.373009	93.158.134.203	192.168.0.130
62	2011-11-24 00:47:55.373009	93.158.134.203	192.168.0.130
63	2011-11-24 00:47:55.380822	93.158.134.203	192.168.0.130
64	2011-11-24 00:47:55.381798	93.158.134.203	192.168.0.130
65	2011-11-24 00:47:55.381798	93.158.134.203	192.168.0.130
66	2011-11-24 00:48:10.238244	192.168.0.130	93.158.134.203
67	2011-11-24 00:48:11.874962	93.158.134.203	192.168.0.130

Frame 67: 423 bytes on wire (3384 bits), 423 bytes captured (3384 bits) on interface 0

- Ethernet II, Src: aa:aa:aa:aa:aa:aa (aa:aa:aa:aa:aa:aa), Dst: 08:00:2b:01:00:00 (08:00:2b:01:00:00)
- Internet Protocol, Src: 93.158.134.203 (93.158.134.203), Dst: 192.168.0.130 (192.168.0.130)
- Transmission Control Protocol, Src Port: http (80), Dst Port: http (80)
- Hypertext Transfer Protocol
  - Line-based text data: text/html
 

```

<html>\r\n
<head><title>302 Found</title></head>\r\n
<body bgcolor="white"AAAAAAAAAAAAAAAAAAAAAAAAAAAA
<center><h1>302 Found</h1></center>\r\n
<hr><center>nginx</center>

```

Text item (text), 51 bytes

Packets: 67 Displayed: 67 Mark...

**Thanks!**

<http://code.google.com/p/windbgshark>

**Questions?**