Windbgshark:

the unified traffic instrumentation tool [1,2,3]

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

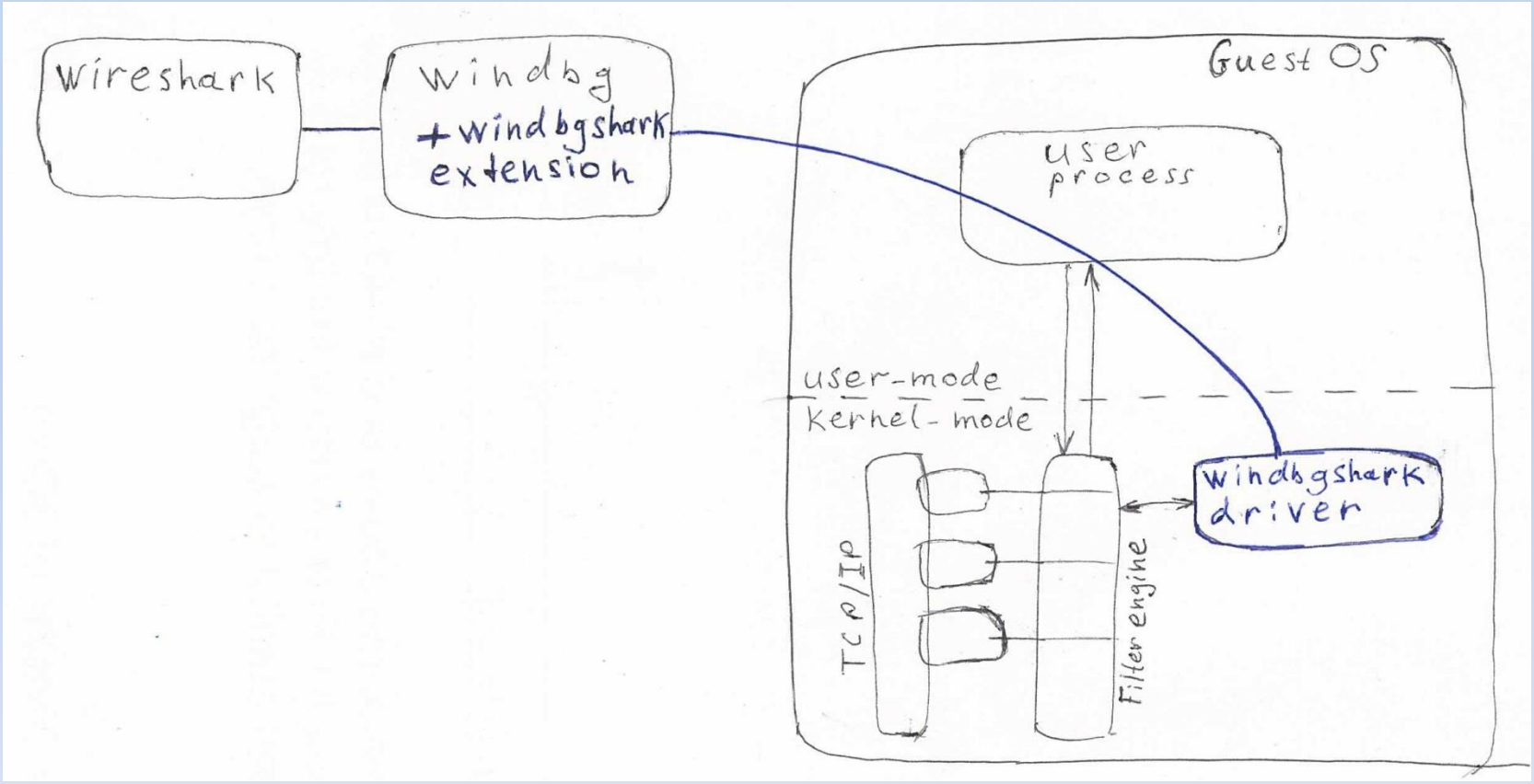
  (reasonable trade-off, TDI on WinXP is almost the same)

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)

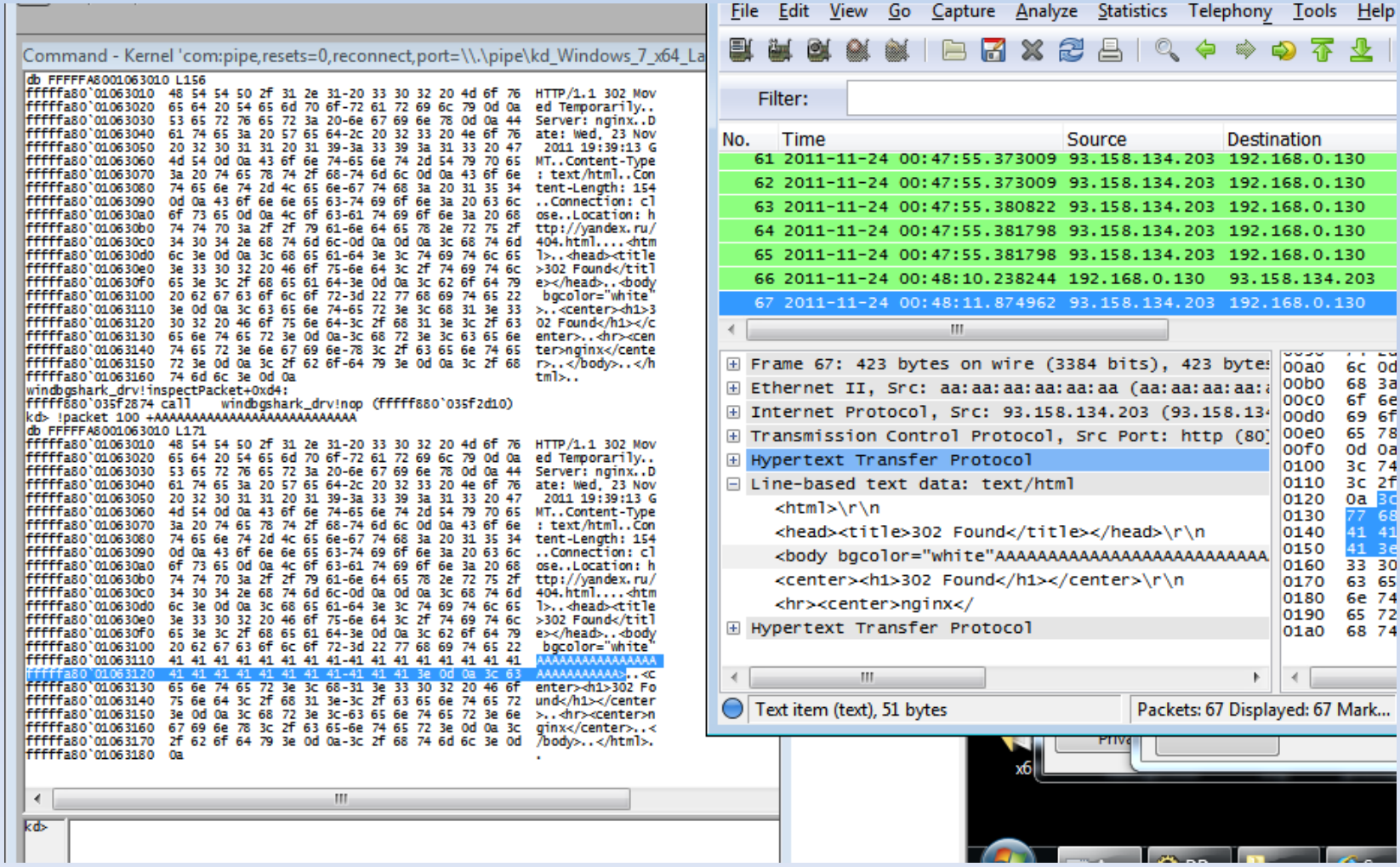
Theory of operation



Quickstart

```
> !load windbgshark
> !strace on
> g
…
> !packet 100 +AAAAAAAAAAAAAAAAAAAA
[look in wireshark]
> g
…
```

Quickstart


Command - Kernel 'com:pipe,resets=0,reconnect,port=\\.\pipe\kd_Windows_7_x64_La
db FFFFFA8001063010 L156
HTTP/1.1 302 Moved Temporarily..
Server: nginx..Date: Wed, 23 Nov 2011 19:39:13 GMT..Content-Type: text/html..Content-Length: 154..Connection: close..Location: http://yandex.ru/404.html....<html><head><title>302 Found</title></head>..<body bgcolor="white">.. <h1>302 Found</h1> ..<hr> nginx ..</body>..</html>..
windbgshark_drv!inspectPacket+0xd4:
kd> !packet 100 +AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
db FFFFFA8001063010 L171
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
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
Ethernet II, Src: aa:aa:aa:aa:aa:aa (aa:aa:aa:aa:aa:aa)
Internet Protocol, Src: 93.158.134.203 (93.158.134.203)
Transmission Control Protocol, Src 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"AAAAAAAAAAAAAAAAAAAAAAAAAA
<h1>302 Found</h1> \r\n
<hr> nginx</
Hypertext Transfer Protocol
Text item (text), 51 bytes
Packets: 67 Displayed: 67 Mark...

Thanks!

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

Questions?