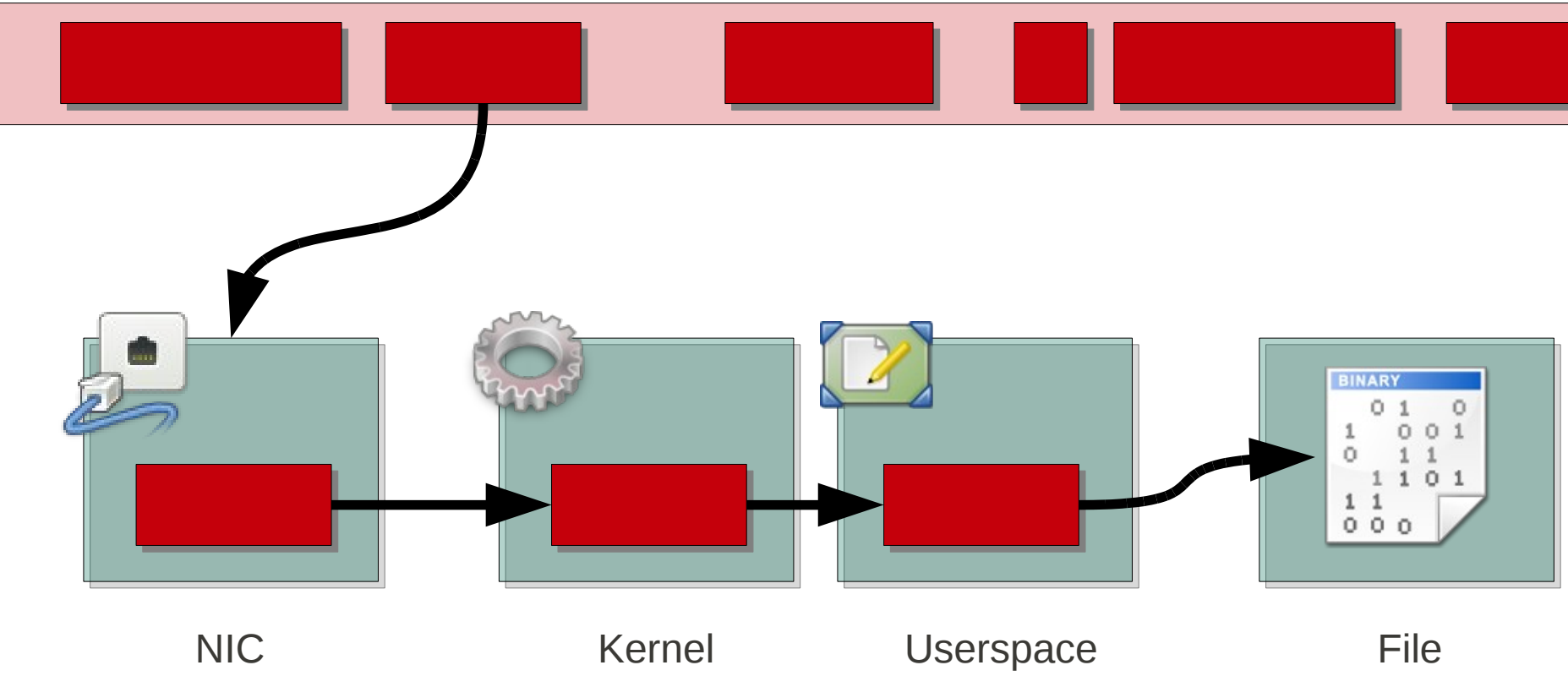
High-Performance Packet Sniffing and Traffic Mining

Tillmann Werner, Senior Virus Analyst, Kaspersky Lab
Honeynet Workshop 2011, Public Day
Paris, 21 March, 2011

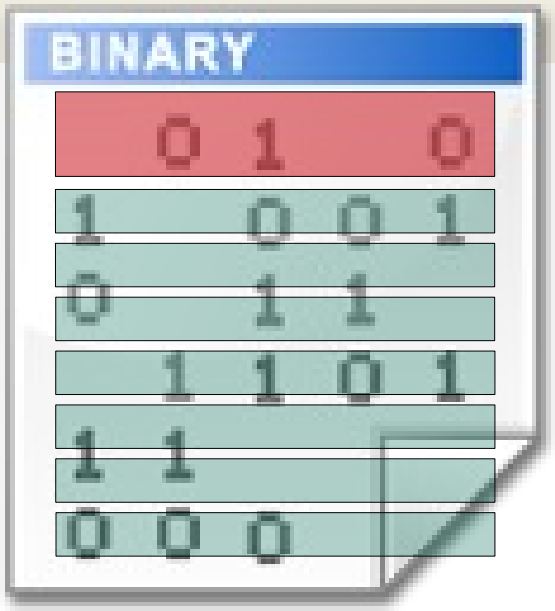
High Performance Packet Sniffing

multicap

Packet Sniffing



The Pcap File Format



Straight-Forward File Format

- Portable library for packet sniffing
- Convenient API for programmers
  - Live capturing
  - Writing and reading dump files
- Open source, GPLv2
- Used by tools like tcpdump, wireshark, snort, …
- Time resolution in microseconds

```
struct pcap_file_header {
        bpf_u_int32 magic;
        u_short version_major;
        u_short version_minor;
        bpf_int32 thiszone;
        bpf_u_int32 sigfigs;
        bpf_u_int32 snaplen;
        bpf_u_int32 linktype;
};
```

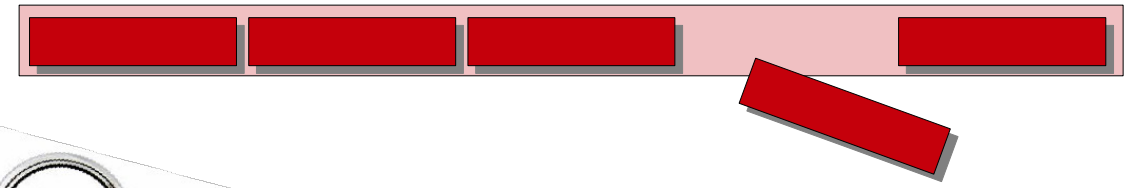
```
struct pcap_pkthdr {
        struct timeval ts;
        bpf_u_int32 caplen;
        bpf_u_int32 len;
};
```


KASPERSKY lab

Do Not Drop The Packets

Packet Drops

- Sniffer too slow: packet drops
- Lost information cannot be recovered
- Missing packets can render TCP streams unusable



Sniffing Performance

- Allocating, copying and freeing memory takes time
- Getting the system time costs CPU cycles
- Reduce such calls as much as possible

Designing *multicap*

Minimize Memory Allocations

- Use a `PF_PACKET` socket
- Attach a user-space ring buffer with `setsockopt(PACKET_RX_RING)`
- This is Linux only

No System Calls To Get Packet Times

- `PF_PACKET` already stores the time stamp in the packet struct
  - nano-second time resolution without further system calls
- No need to call `localtime()` etc.

Memory-mapped Dump Files

- `mmap()` for increased dumping
- Pre-allocate multiples of page size

Configuration Example

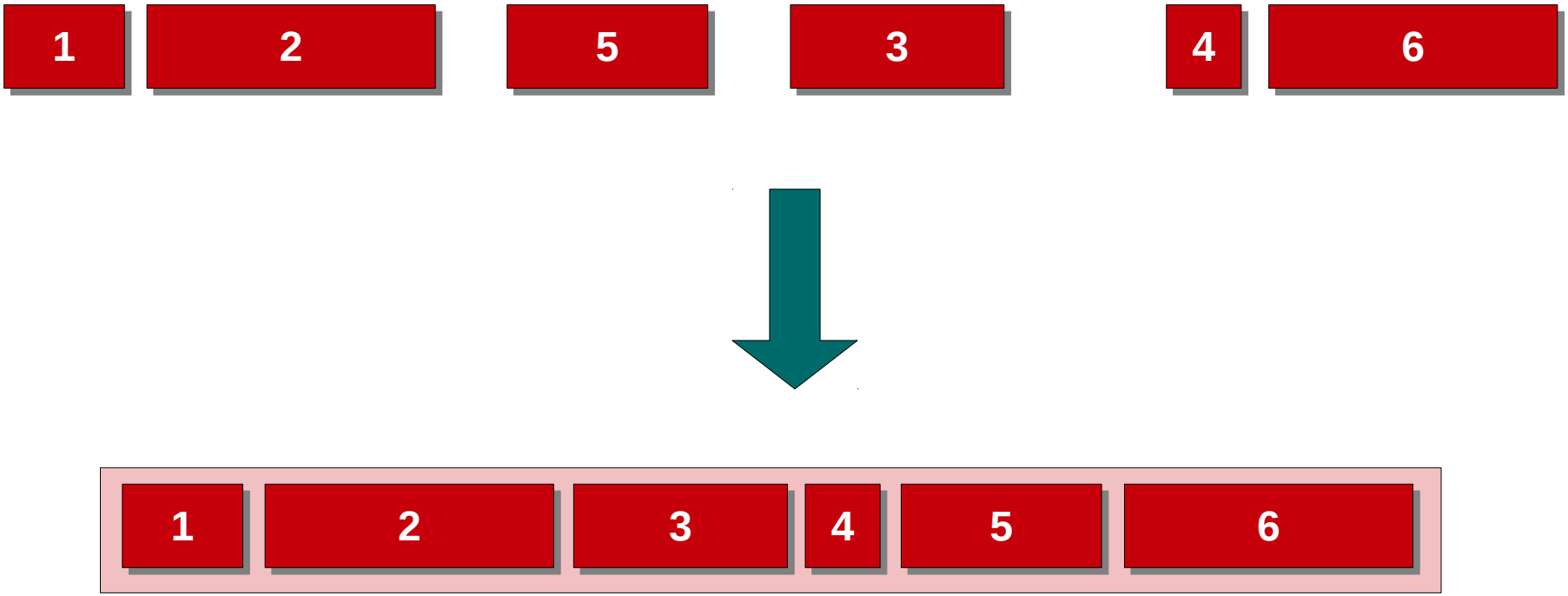
```
rotate = "1d" // "h|d|G|M"
path = ""
file = "$tracker-%Y%m%d.pcap"

trackers = {
        tcponly =
        {
                enabled = "true"
                interface = "eth0"
                bpf = "tcp"
                snaplen = "0"
                rotate = "10M"
                path = "var/log/multicap/$tracker/%Y-%m-%d"
                file = "%H:%M:%S.pcap"
                promisc = "0"
        }
}
```

multicap Demo

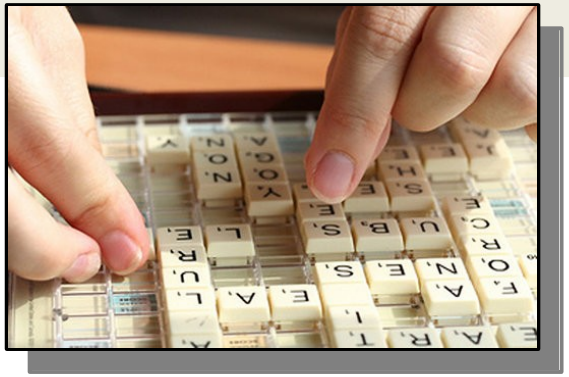
Packet Trace File Processing

streams

Stream Reassembly



TCP Stream Reassembly

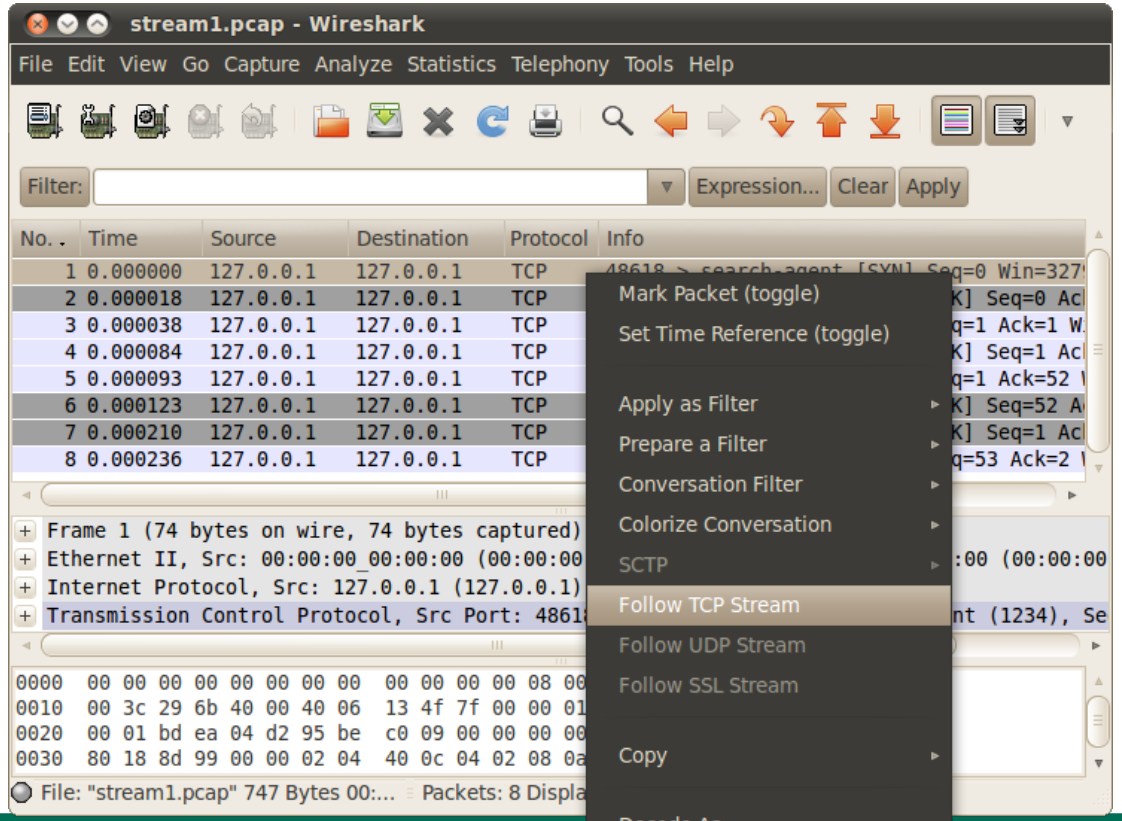


TCP Streams

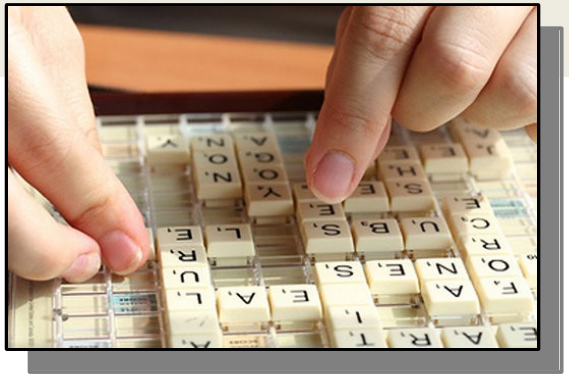
- Stream: reliable, ordered stream of data
- OS assembles segments in the right order

Stream Reassembly Tools

- Wireshark
- tcpick
- tcpflow



TCP Stream Reassembly

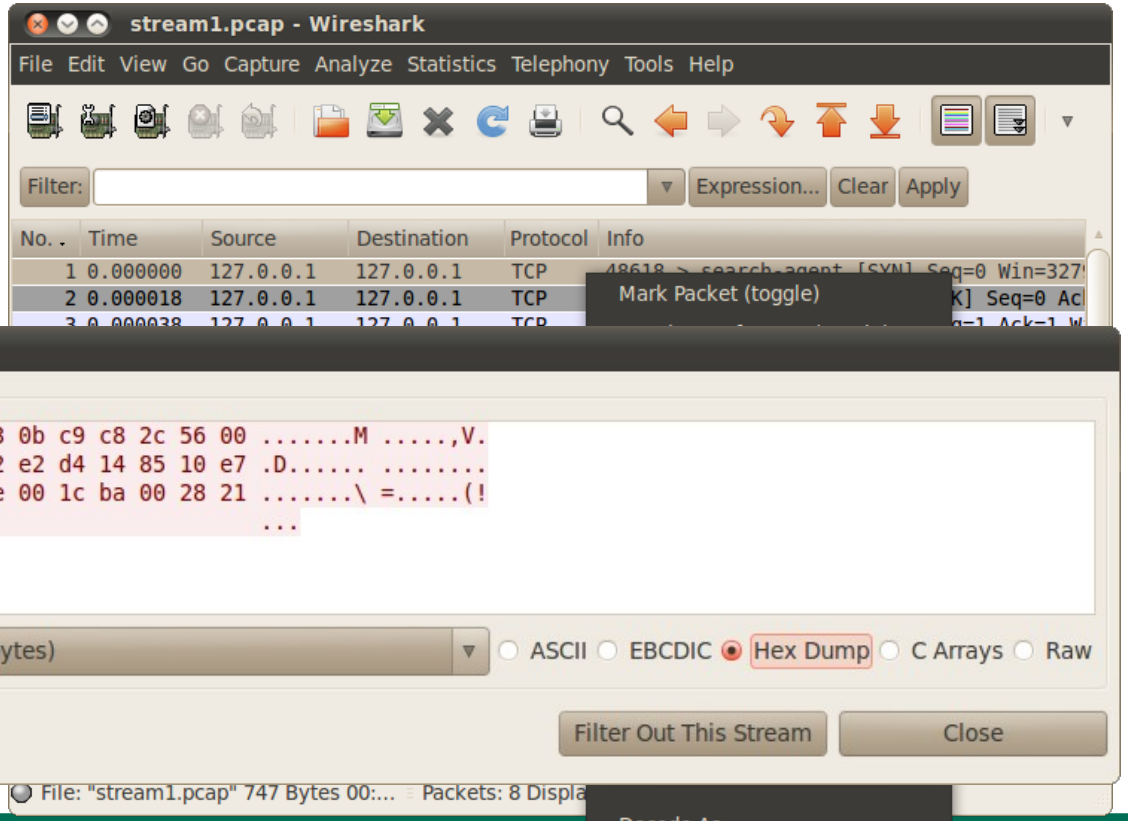


TCP Streams

- Stream: reliable, ordered stream of data
- OS assembles segments in the right order

Stream Reassembly Tools

- Wireshark
- tcpick
- tcpflow



Designing *streams*

Stream

- IP addresses, port numbers, initial sequence number

Stream Reassembly Strategy

- A SYN segment starts a new stream
- A RST or FIN segment terminates a stream
- Any segment gets copied at the right offset according to its sequence number

Interactive Command Line Tool

- Listing, counting, filtering, selecting, … streams
- Easy integration of external tools

Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection

<**http://insecure.org/stf/secnet_ids/secnet_ids.html**>

streams Demo

Code

Where To Get Them

```
lftp anonymous@ftp.carnivore.it:/> cd projects/streams/
lftp anonymous@ftp.carnivore.it:/projects/streams> ls
-rw-r--r--    1 33       33         125549 Mar 16 16:19 streams-0.1.0.tar.bz2
-rw-r--r--    1 33       33         235740 Mar 16 16:19 streams-0.1.0.tar.gz
lftp anonymous@ftp.carnivore.it:/projects/streams>
```

git carnivore.it code browser

source web interface to carnivore.it projects

index

Name	Description
projects	
carniwwwhore	webif for dionaeas xmpp fed postgres database
dionaea	low interaction honeypot - our nepenthes sucessor
honeytrap	low interaction honeypot - the attacker implements the protocol
libemu	x86 emulation library to detect and emulate shellcode
liblcfg	lightweight configuration parsing library
libxmatch	library for matching patterns in xor-encoded data.
multicap	multi interface networkstream dump daemon
nebula	attack signtures via clustering
nepenthes	low interaction honeypot - use dionaea instead
pehunter	snort plugin to carve PE files from network streams
regoogle	google assisted reverse engeneering
streams	Play with pcap files
users	
users/common/aguri	aguri fork for the ladies
users/common/prosody	prosody fork with sensor network patches
users/gento/dionaea	dionaea branch for new things
users/phibo/dionaea	dionaea branch for reason

http://src.carnivore.it

ftp.carnivore.it

Thank You

High-Performance Packet Sniffing and Traffic Mining

Tillmann Werner, Senior Virus Analyst, Kaspersky Lab
Honeynet Workshop 2011, Public Day
Paris, 21 March, 2011