Tracedump: A Novel Single Application IP Packet Sniffer

Paweł Foremski, IITiS PAN
pjf@iitis.pl

3rd TMA PhD School
AGH, Kraków 2012

IITiS

Hello!

- Paweł (Paul)
- MSc since 2011
- Institute of Theoretical and Applied Informatics of the Polish Academy of Sciences
- Gliwice, Poland

Interests

- Simulation of wireless networks
- Network security
- Traffic classification
  - MSc - implementation of KISS
  - Research grant from the Polish National Science Centre – project **MuTriCs**

MuTriCs

- **MU**ltilevel **TR**aff**i**c **C**la**S**sification in the Internet
- 2011 – 2013
- Research supervisor: prof. Michele Pagano, University of Pisa
- http://mutrics.iitis.pl

MuTriCs

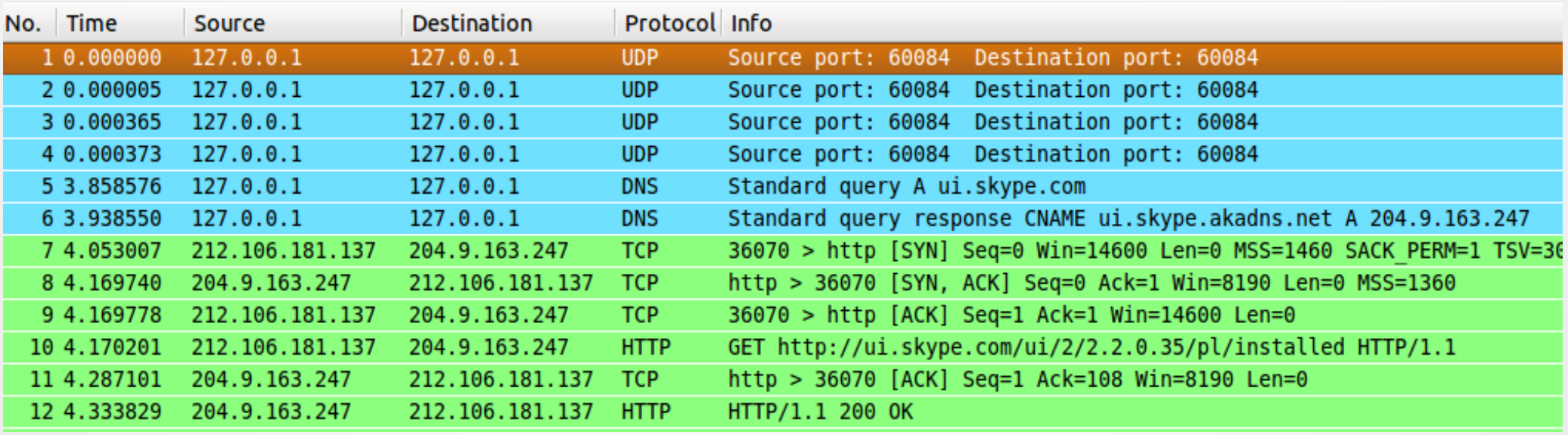
- Real-time IP traffic classification system
- **Integration of traffic features on many levels**
- Expected results
  - Detailed and reliable classification
  - Anomaly detection
  - Open source software for traffic analysis

- Currently preparing the tools: tracedump

The idea

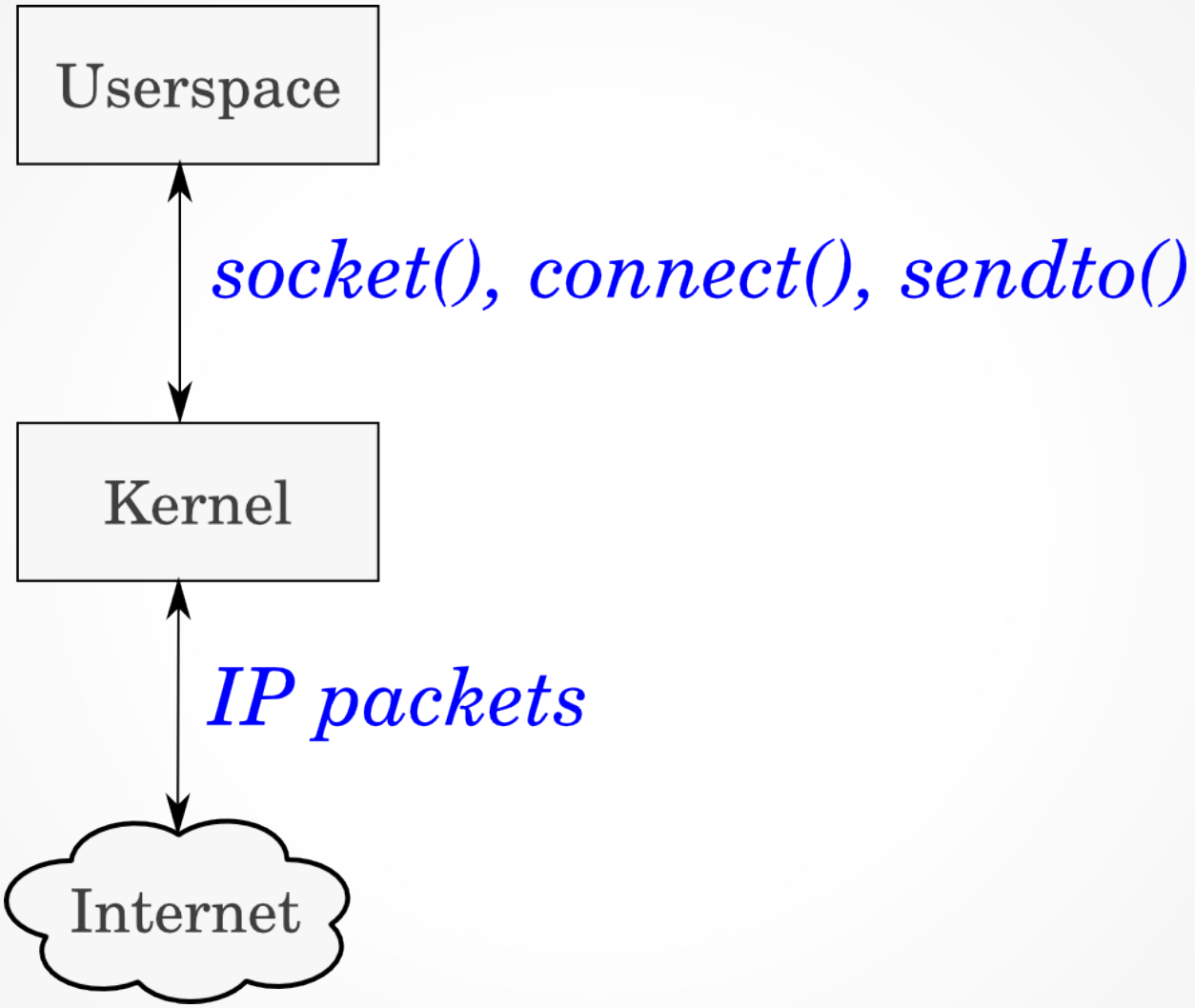
Tracedump: single application sniffer for Linux

```
# tracedump -w out.pcap skype
# wireshark ./out.pcap
```

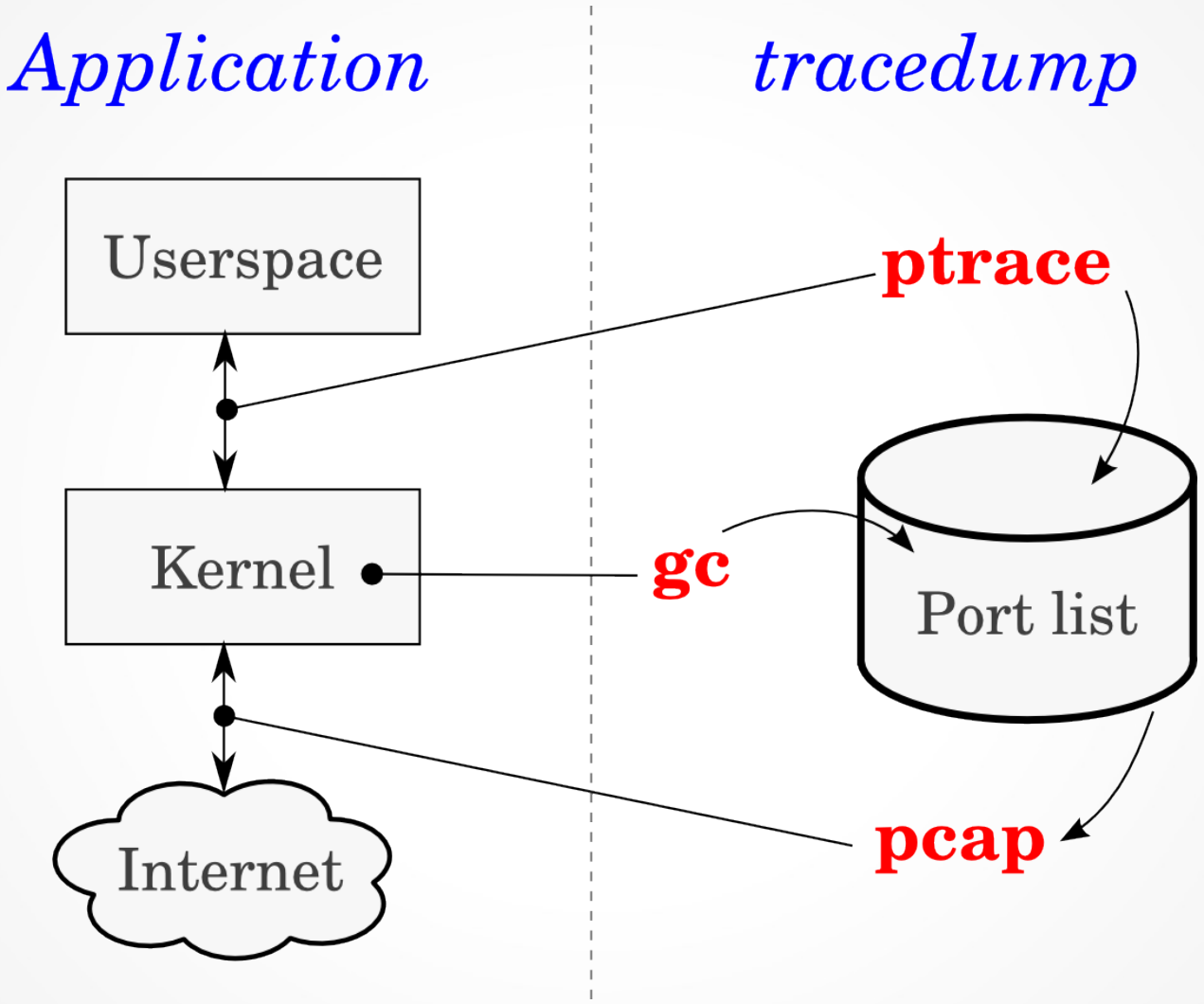


No.	Time	Source	Destination	Protocol	Info
1	0.000000	127.0.0.1	127.0.0.1	UDP	Source port: 60084 Destination port: 60084
2	0.000005	127.0.0.1	127.0.0.1	UDP	Source port: 60084 Destination port: 60084
3	0.000365	127.0.0.1	127.0.0.1	UDP	Source port: 60084 Destination port: 60084
4	0.000373	127.0.0.1	127.0.0.1	UDP	Source port: 60084 Destination port: 60084
5	3.858576	127.0.0.1	127.0.0.1	DNS	Standard query A ui.skype.com
6	3.938550	127.0.0.1	127.0.0.1	DNS	Standard query response CNAME ui.skype.akadns.net A 204.9.163.247
7	4.053007	212.106.181.137	204.9.163.247	TCP	36070 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSV=30
8	4.169740	204.9.163.247	212.106.181.137	TCP	http > 36070 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1360
9	4.169778	212.106.181.137	204.9.163.247	TCP	36070 > http [ACK] Seq=1 Ack=1 Win=14600 Len=0
10	4.170201	212.106.181.137	204.9.163.247	HTTP	GET http://ui.skype.com/ui/2/2.2.0.35/pl/installed HTTP/1.1
11	4.287101	204.9.163.247	212.106.181.137	TCP	http > 36070 [ACK] Seq=1 Ack=108 Win=8190 Len=0
12	4.333829	204.9.163.247	212.106.181.137	HTTP	HTTP/1.1 200 OK

TCP connection



Architecture



Motivation

- Quick and simple IP trace extraction
- Convenient way to analyze new applications
- No such tool

- Vision: *automatic traffic generation and collection*
  - Scripts
  - GUI testing tools
  - Can run for many hours
  - Sharing

Classification: pros

- **Pure** and **complete** traffic samples
- Reliable, detailed ground truth
- Full packet payload
- Real-time
- Quick and simple

Classification: cons

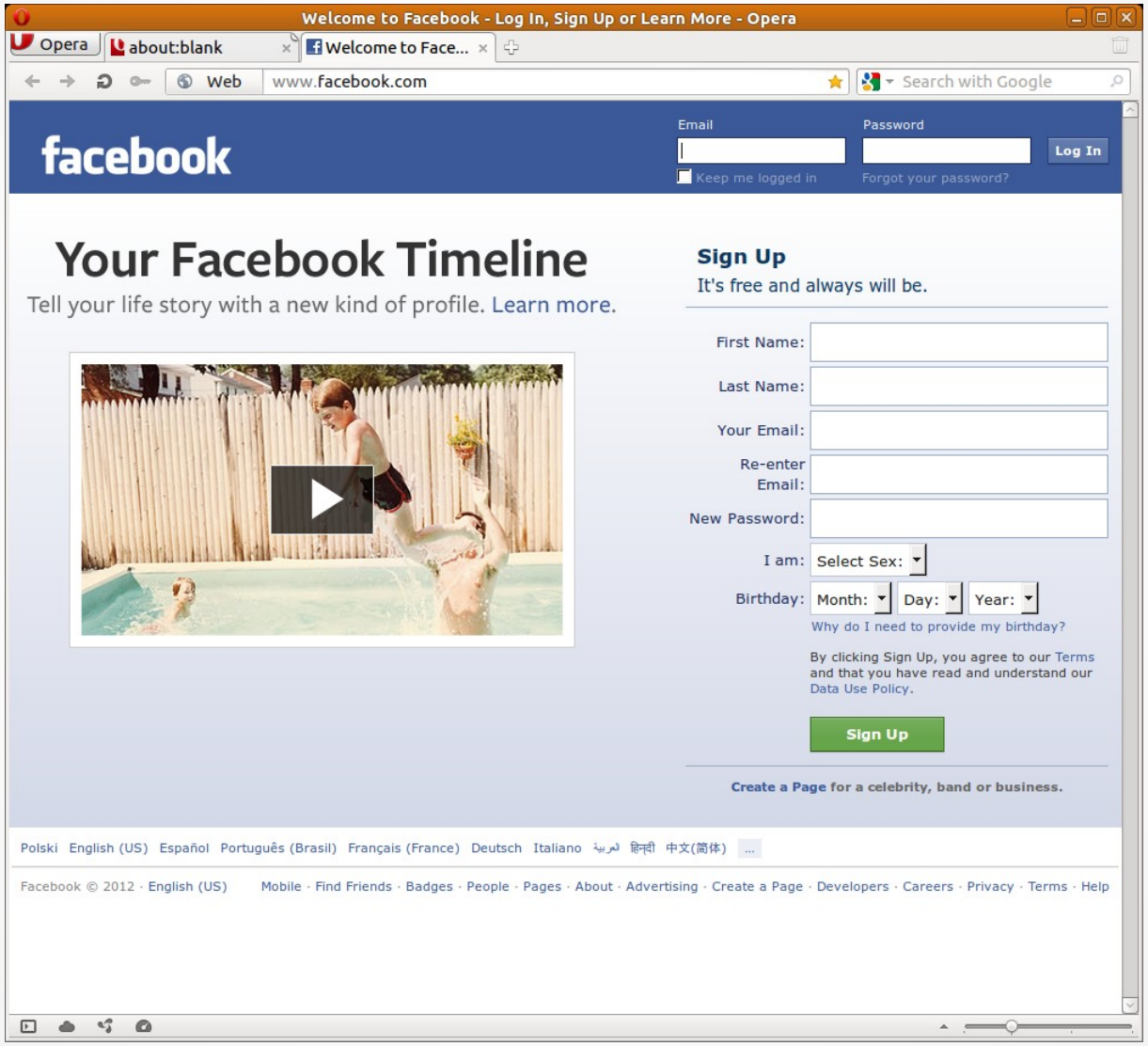
- Synthetic traces
- Comparing to the scale of global Internet:
  - small amounts of data
  - small range of observable applications

Applications

- Supplementary to “real” data traces
- Rapid generation of interim training data for machine learning algorithms
- Ad-hoc experiments
- Insight into “side channels” of network protocols and applications

Example: Opera 11

```
tracedump opera www.facebook.com
```



Opera: startup

No.	Time	Source	Destination	Protocol	Info
1	0.000000	212.106.181.137	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
2	0.000104	212.106.181.137	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
3	0.000201	212.106.181.137	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
4	0.000820	212.106.181.137	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
5	0.000884	212.106.181.137	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
6	0.000943	212.106.181.137	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
7	0.001685	192.168.88.253	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
8	0.001753	192.168.88.253	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
9	0.001817	192.168.88.253	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
10	0.002367	192.168.1.253	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
11	0.002434	192.168.1.253	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
12	0.002499	192.168.1.253	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
13	0.003261	192.168.2.1	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
14	0.003325	192.168.2.1	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
15	0.003380	192.168.2.1	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1

```
▷ Frame 1: 188 bytes on wire (1504 bits), 188 bytes captured (1504 bits)
▷ Linux cooked capture
▷ Internet Protocol, Src: 212.106.181.137 (212.106.181.137), Dst: 239.255.255.250 (239.255.255.250)
▷ User Datagram Protocol, Src Port: 49323 (49323), Dst Port: ssdp (1900)
▽ Hypertext Transfer Protocol
  ▷ M-SEARCH * HTTP/1.1\r\n
    HOST: 239.255.255.250:1900\r\n
    ST: urn:opera-com:device:OperaUnite:1\r\n
    MAN: "ssdp:discover"\r\n
    MX: 3\r\n
    User-Agent: Opera Unite\r\n
    \r\n
```

Opera: site check

No.	Time	Source	Destination	Protocol	Info
16	0.466622	127.0.0.1	127.0.0.1	DNS	Standard query A www.facebook.com
17	0.466689	127.0.0.1	127.0.0.1	DNS	Standard query response A 66.220.156.64
18	0.701476	212.106.181.137	66.220.156.64	TCP	37498 > http [SYN] Seq=0 Win=14600 Len=0
19	0.710628	127.0.0.1	127.0.0.1	DNS	Standard query A sitecheck2.opera.com
20	0.790230	127.0.0.1	127.0.0.1	DNS	Standard query response A 91.203.99.45
21	0.791319	212.106.181.137	91.203.99.45	TCP	44034 > http [SYN] Seq=0 Win=14600 Len=0
22	0.824398	66.220.156.64	212.106.181.137	TCP	http > 37498 [SYN, ACK] Seq=0 Ack=1 Win=4
23	0.824433	212.106.181.137	66.220.156.64	TCP	37498 > http [ACK] Seq=1 Ack=1 Win=14600
24	0.825166	212.106.181.137	66.220.156.64	HTTP	GET / HTTP/1.1
25	0.827488	91.203.99.45	212.106.181.137	TCP	http > 44034 [SYN, ACK] Seq=0 Ack=1 Win=4
26	0.827515	212.106.181.137	91.203.99.45	TCP	44034 > http [ACK] Seq=1 Ack=1 Win=14600
27	0.828025	212.106.181.137	91.203.99.45	HTTP	GET /?host=www.facebook.com&hdn=UhGTse4BN

More information

mutrics.iitis.pl/tracedump

(GNU GPL)

Foremski P., "***Tracedump: A Novel Single Application IP Packet Sniffer***", Theoretical and Applied Informatics, Vol. 24 No. 1/2012

Future work

- Implementation:
  - Stability, Linux 64-bit
  - Port limit (300)
- Methodology:
  - GUI automation
  - Automatic traffic trace collection
- **Practical applications in the MuTriCs project**

Thank you!

mutrics.iitis.pl