University of Amsterdam

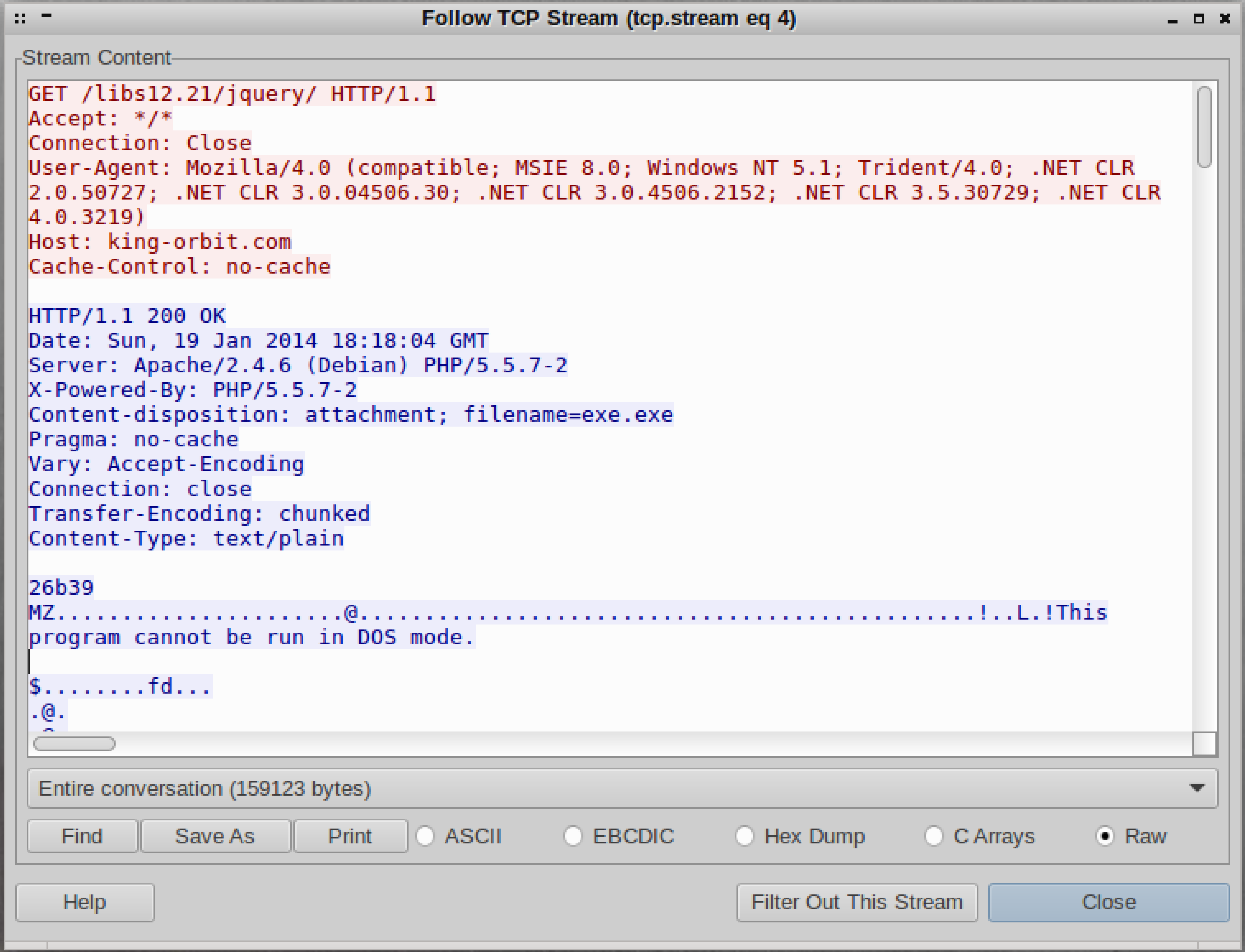
Online event registration with minimal privacy violation

Research project nr. 2 – presentation

Niels van Dijkhuizen

Introduction

Sharing captured network data

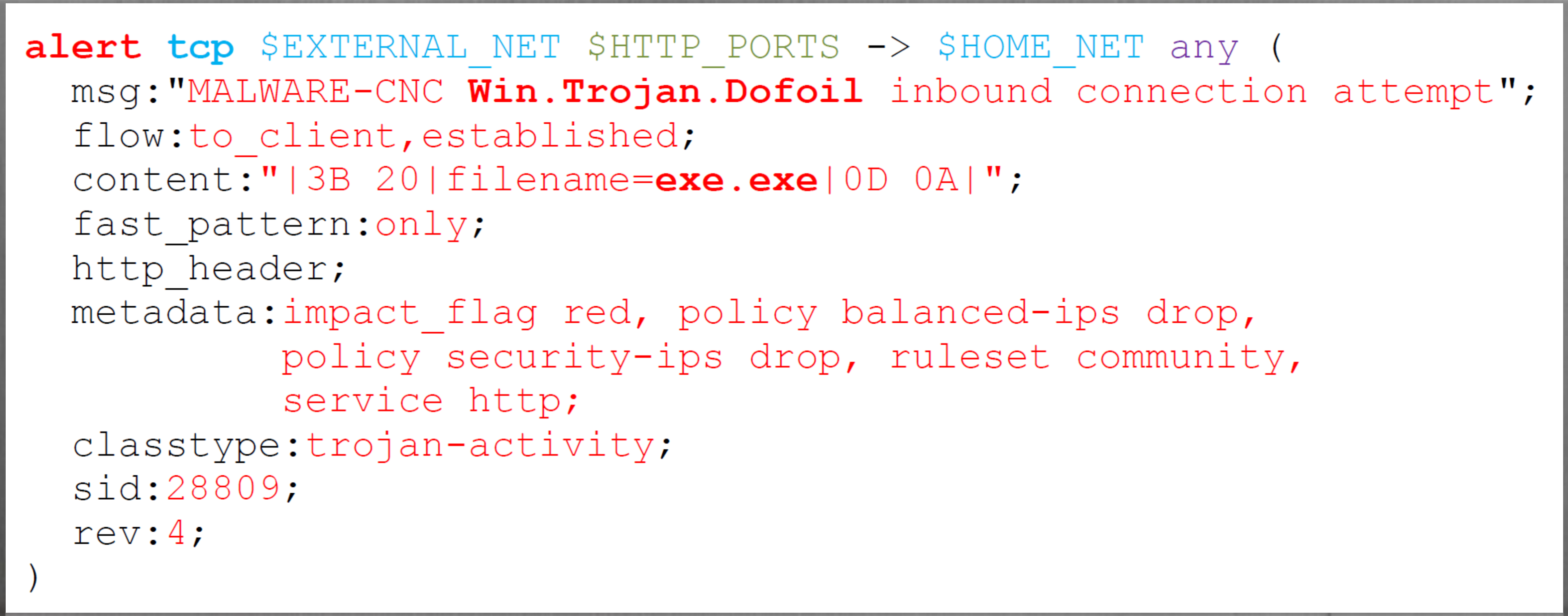


```
GET /libs12.21/jquery/ HTTP/1.1
Accept: */*
Connection: Close
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR
2.0.50727; .NET CLR 3.0.04506.30; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET CLR
4.0.3219)
Host: king-orbit.com
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Sun, 19 Jan 2014 18:18:04 GMT
Server: Apache/2.4.6 (Debian) PHP/5.5.7-2
X-Powered-By: PHP/5.5.7-2
Content-disposition: attachment; filename=exe.exe
Pragma: no-cache
Vary: Accept-Encoding
Connection: close
Transfer-Encoding: chunked
Content-Type: text/plain

26b39
MZ......................@...............................................!..L.!This
program cannot be run in DOS mode.

$........fd...
.@.
```

Entire conversation (159123 bytes)

Find | Save As | Print | ○ ASCII | ○ EBCDIC | ○ Hex Dump | ○ C Arrays | ● Raw

IDS rule



```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (
  msg:"MALWARE-CNC Win.Trojan.Dofoil inbound connection attempt";
  flow:to_client,established;
  content:"|3B 20|filename=exe.exe|0D 0A|";
  fast_pattern:only;
  http_header;
  metadata:impact_flag red, policy balanced-ips drop,
           policy security-ips drop, ruleset community,
           service http;
  classtype:trojan-activity;
  sid:28809;
  rev:4;
)
```

Privacy concerns

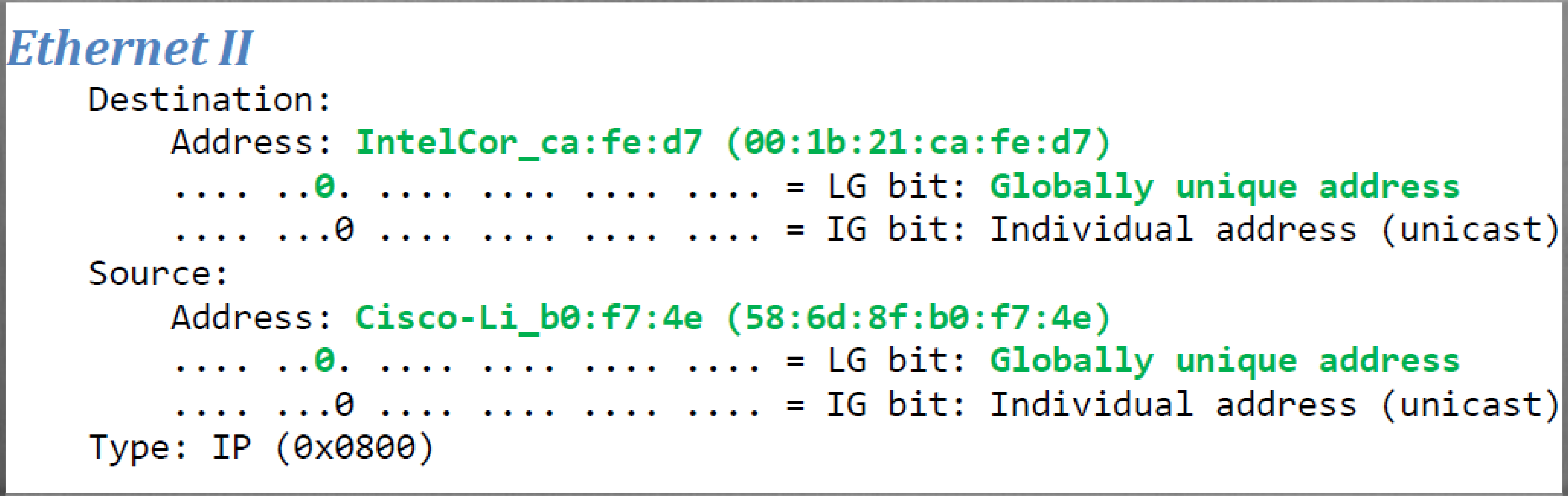
Image source: www.birminghamavs.com/tag/surveillance-cameras

Research Question

> *Is it possible to create a system that indicates network threats with minimal privacy violation?*

Approach

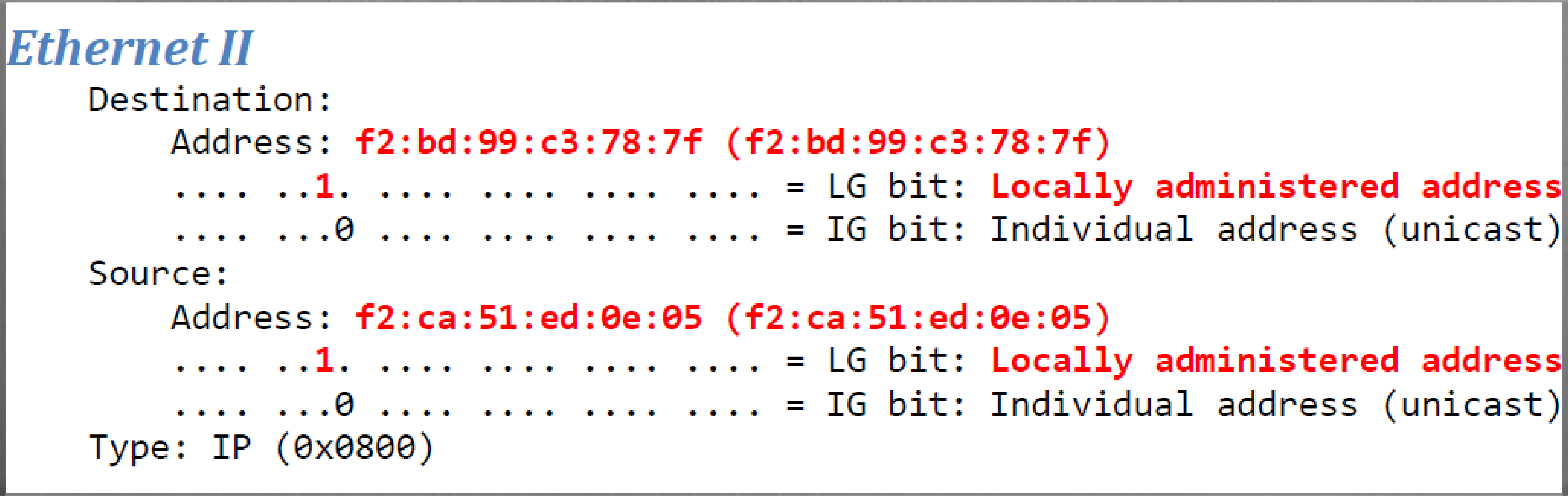
Anonymisation example 1



Ethernet II

```
Destination:
    Address: IntelCor_ca:fe:d7 (00:1b:21:ca:fe:d7)
    .... ..0. .... .... .... .... = LG bit: Globally unique address
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Source:
    Address: Cisco-Li_b0:f7:4e (58:6d:8f:b0:f7:4e)
    .... ..0. .... .... .... .... = LG bit: Globally unique address
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Type: IP (0x0800)
```

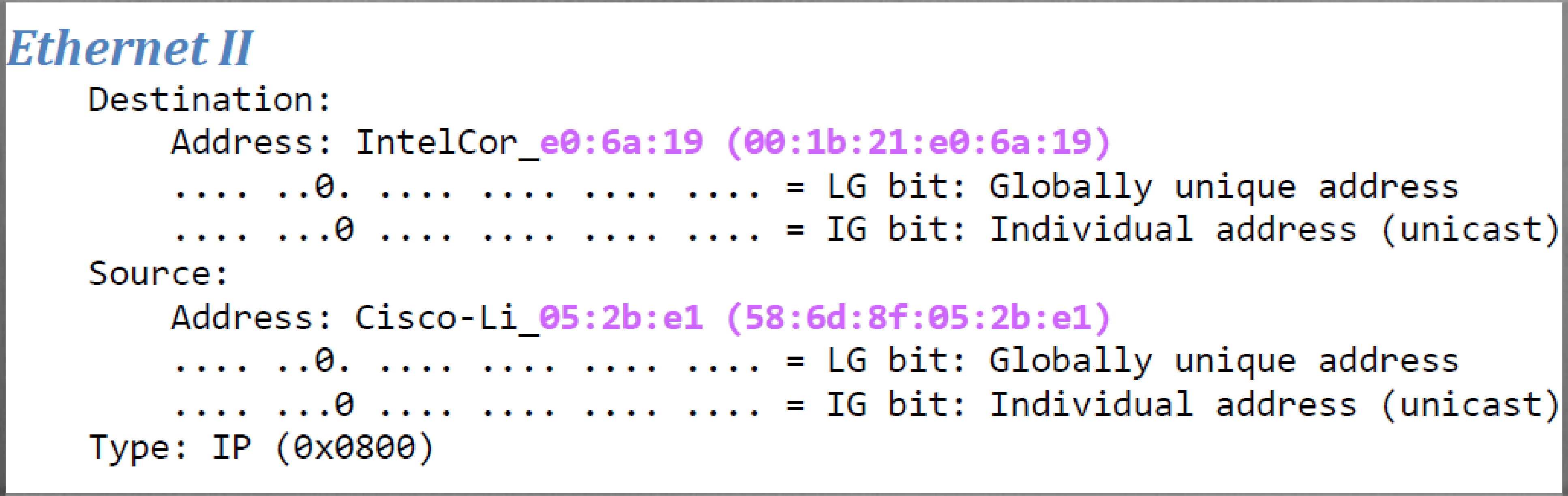
Anonymisation example 1



Ethernet II

```
Destination:
    Address: f2:bd:99:c3:78:7f (f2:bd:99:c3:78:7f)
    .... ..1. .... .... .... .... = LG bit: Locally administered address
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Source:
    Address: f2:ca:51:ed:0e:05 (f2:ca:51:ed:0e:05)
    .... ..1. .... .... .... .... = LG bit: Locally administered address
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Type: IP (0x0800)
```

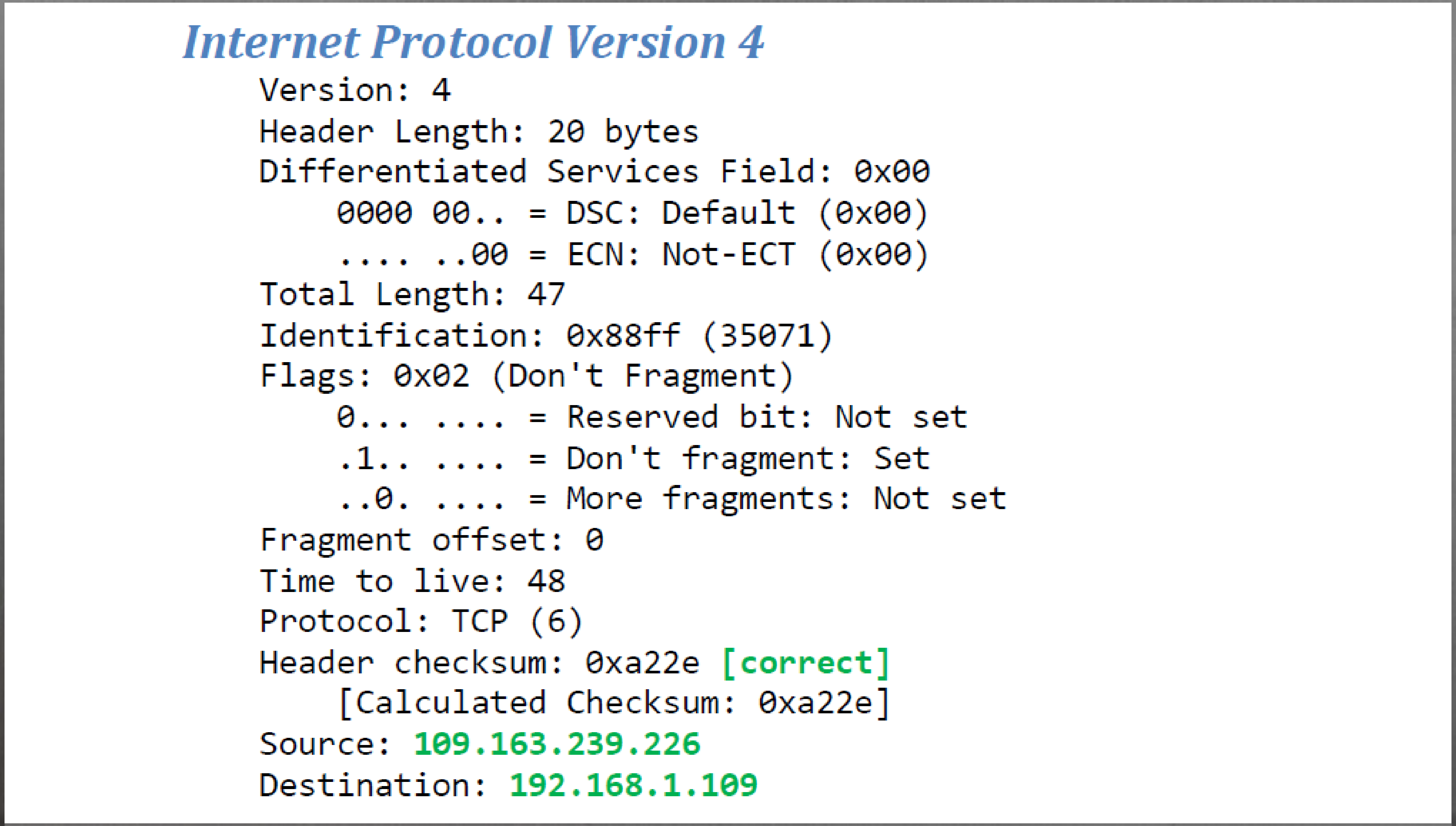
Anonymisation example 1



Ethernet II

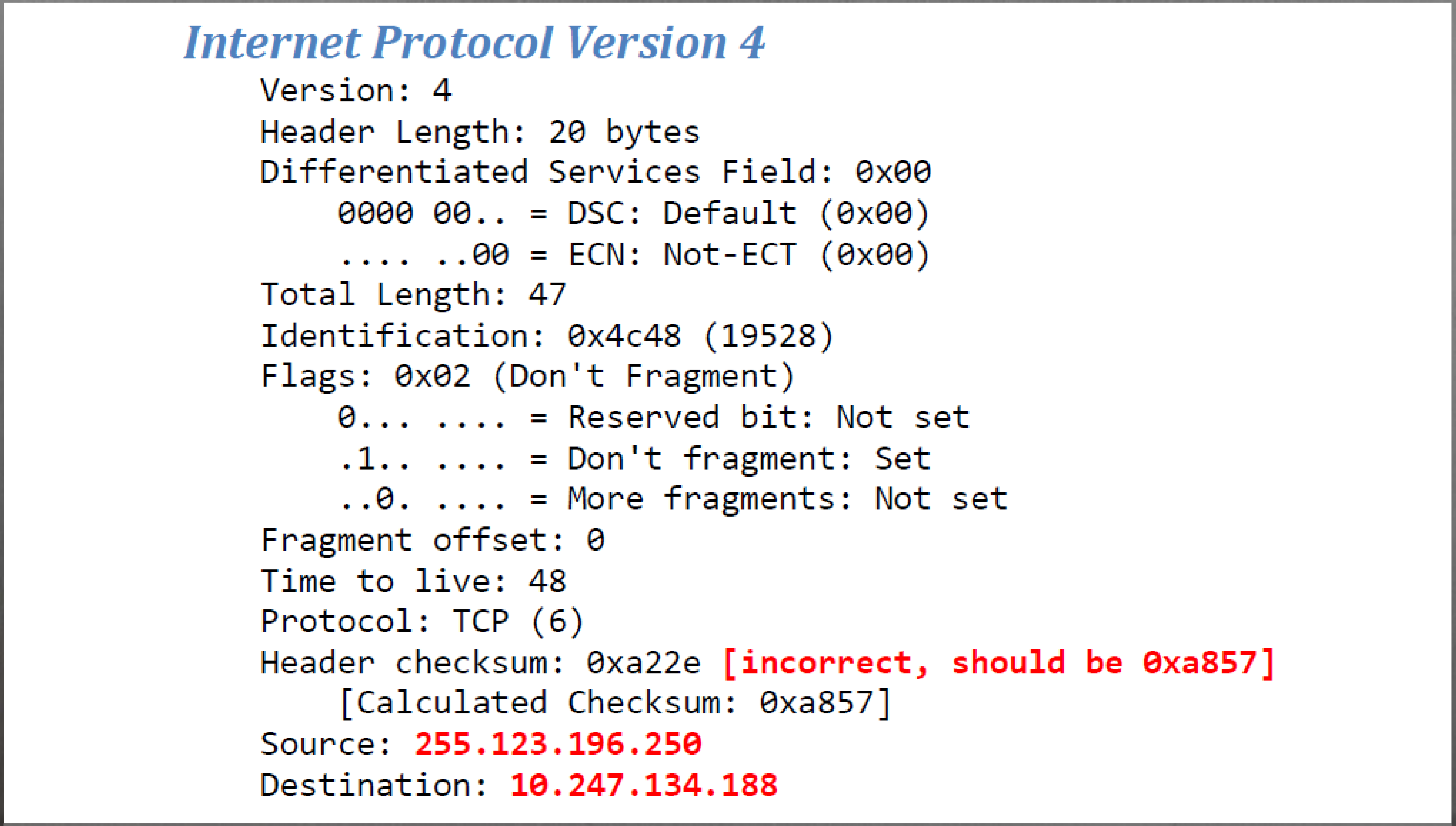
```
    Destination:
        Address: IntelCor_e0:6a:19 (00:1b:21:e0:6a:19)
        .... ..0. .... .... .... .... = LG bit: Globally unique address
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source:
        Address: Cisco-Li_05:2b:e1 (58:6d:8f:05:2b:e1)
        .... ..0. .... .... .... .... = LG bit: Globally unique address
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IP (0x0800)
```

Anonymisation example 2



```
Internet Protocol Version 4
    Version: 4
    Header Length: 20 bytes
    Differentiated Services Field: 0x00
        0000 00.. = DSC: Default (0x00)
        .... ..00 = ECN: Not-ECT (0x00)
    Total Length: 47
    Identification: 0x88ff (35071)
    Flags: 0x02 (Don't Fragment)
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 48
    Protocol: TCP (6)
    Header checksum: 0xa22e [correct]
        [Calculated Checksum: 0xa22e]
    Source: 109.163.239.226
    Destination: 192.168.1.109
```

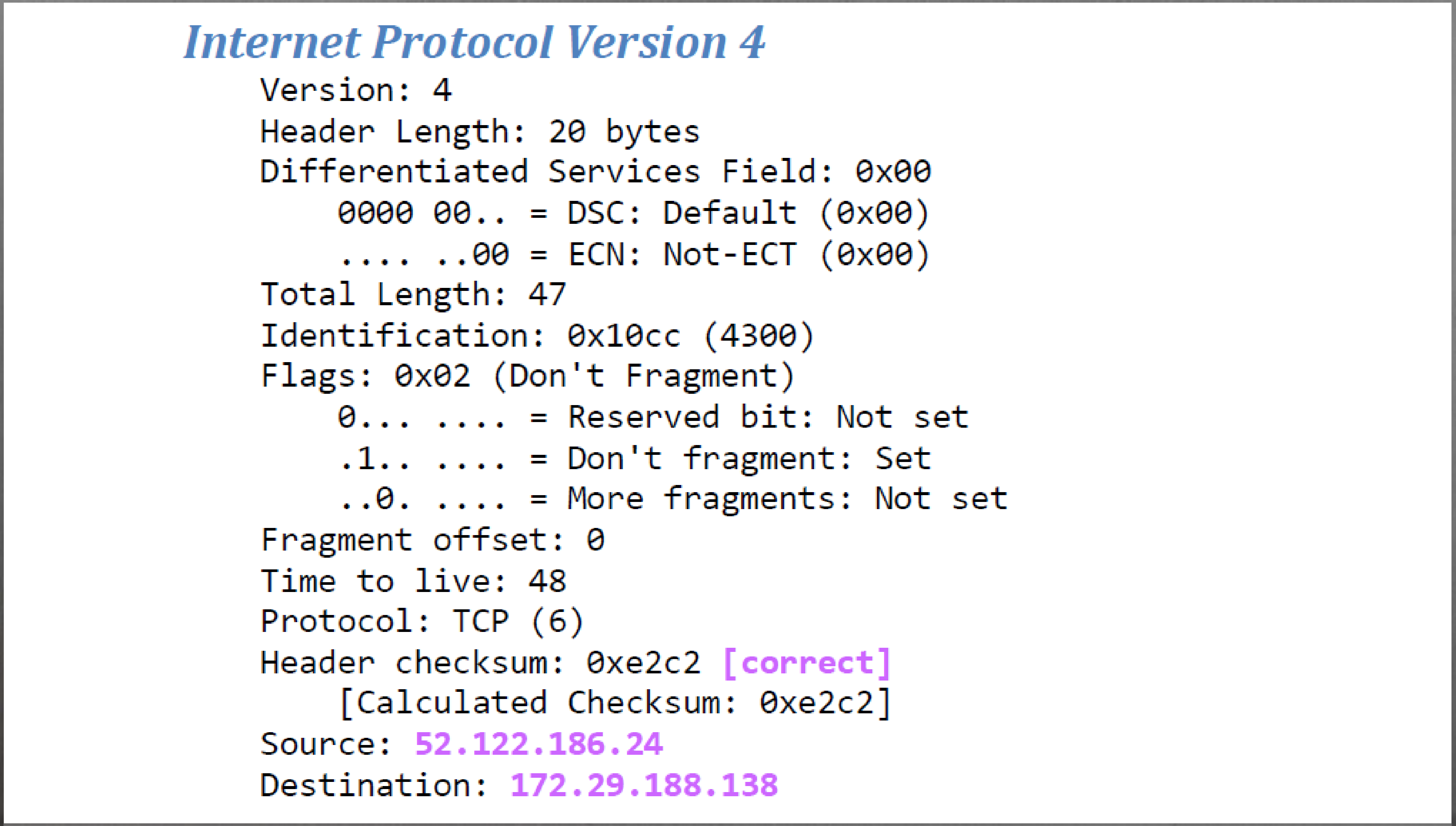
Anonymisation example 2



Internet Protocol Version 4

```
Version: 4
Header Length: 20 bytes
Differentiated Services Field: 0x00
    0000 00.. = DSC: Default (0x00)
    .... ..00 = ECN: Not-ECT (0x00)
Total Length: 47
Identification: 0x4c48 (19528)
Flags: 0x02 (Don't Fragment)
    0... .... = Reserved bit: Not set
    .1.. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
Fragment offset: 0
Time to live: 48
Protocol: TCP (6)
Header checksum: 0xa22e [incorrect, should be 0xa857]
    [Calculated Checksum: 0xa857]
Source: 255.123.196.250
Destination: 10.247.134.188
```

Anonymisation example 2



```
Internet Protocol Version 4
    Version: 4
    Header Length: 20 bytes
    Differentiated Services Field: 0x00
        0000 00.. = DSC: Default (0x00)
        .... ..00 = ECN: Not-ECT (0x00)
    Total Length: 47
    Identification: 0x10cc (4300)
    Flags: 0x02 (Don't Fragment)
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 48
    Protocol: TCP (6)
    Header checksum: 0xe2c2 [correct]
        [Calculated Checksum: 0xe2c2]
    Source: 52.122.186.24
    Destination: 172.29.188.138
```

Techniques and concepts

- Anonymisation or Pseudonymisation?
- Transformation primitives

Image source: www.open.edu/openlearn/society/the-white-mask

Inference attacks

- Passive fingerprinting to infer objects and topology
- Active Data injection attack (chosen plaintext)
- Cryptographic attacks
- Even PETs are not safe!

source: www.grumpycats.com

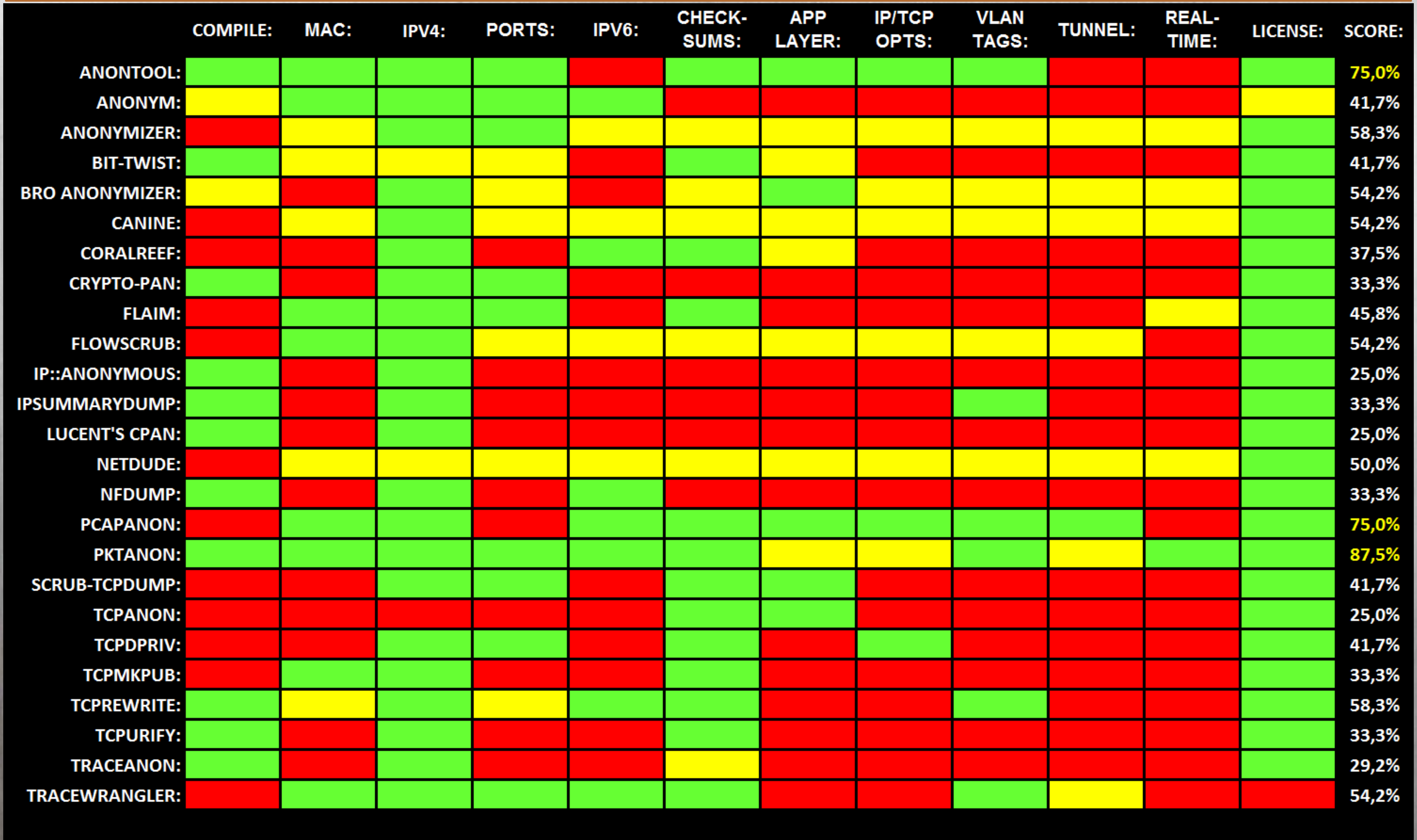
Requirements of the Anonymisation system

- Full support for Link-, Internet- and Transport layers;

- Features for application layer anonymisation;

- Real time processing network streams.

State of current tools



	COMPILE:	MAC:	IPV4:	PORTS:	IPV6:	CHECK-SUMS:	APP LAYER:	IP/TCP OPTS:	VLAN TAGS:	TUNNEL:	REAL-TIME:	LICENSE:	SCORE:
ANONTOOL:	🟩	🟩	🟩	🟩	🟥	🟩	🟩	🟩	🟩	🟥	🟥	🟩	75,0%
ANONYM:	🟨	🟩	🟩	🟩	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟨	41,7%
ANONYMIZER:	🟥	🟨	🟩	🟩	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟩	58,3%
BIT-TWIST:	🟩	🟨	🟨	🟨	🟥	🟩	🟨	🟥	🟥	🟥	🟥	🟩	41,7%
BRO ANONYMIZER:	🟨	🟥	🟩	🟨	🟥	🟨	🟩	🟨	🟨	🟨	🟨	🟩	54,2%
CANINE:	🟥	🟨	🟩	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟩	54,2%
CORALREEF:	🟥	🟥	🟩	🟥	🟩	🟩	🟨	🟥	🟥	🟥	🟥	🟩	37,5%
CRYPTO-PAN:	🟩	🟥	🟩	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	33,3%
FLAIM:	🟥	🟩	🟩	🟩	🟥	🟩	🟥	🟥	🟥	🟥	🟨	🟩	45,8%
FLOWSCRUB:	🟥	🟩	🟩	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟥	🟩	54,2%
IP::ANONYMOUS:	🟩	🟥	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	25,0%
IPSUMMARYDUMP:	🟩	🟥	🟩	🟥	🟥	🟥	🟥	🟥	🟩	🟥	🟥	🟩	33,3%
LUCENT'S CPAN:	🟩	🟥	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	25,0%
NETDUDE:	🟥	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟩	50,0%
NFDUMP:	🟩	🟥	🟩	🟥	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟩	33,3%
PCAPANON:	🟥	🟩	🟩	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟩	75,0%
PKTANON:	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟨	🟩	🟩	87,5%
SCRUB-TCPDUMP:	🟥	🟥	🟩	🟩	🟥	🟩	🟩	🟥	🟥	🟥	🟥	🟩	41,7%
TCPANON:	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟥	🟥	🟥	🟥	🟩	25,0%
TCPDPRIV:	🟥	🟥	🟩	🟩	🟥	🟩	🟥	🟩	🟥	🟥	🟥	🟩	41,7%
TCPMKPUB:	🟥	🟩	🟩	🟥	🟥	🟩	🟥	🟥	🟥	🟥	🟥	🟩	33,3%
TCPREWRITE:	🟩	🟨	🟩	🟨	🟩	🟩	🟥	🟥	🟩	🟥	🟥	🟩	58,3%
TCPURIFY:	🟩	🟥	🟩	🟥	🟥	🟩	🟥	🟥	🟥	🟥	🟥	🟩	33,3%
TRACEANON:	🟩	🟥	🟩	🟥	🟥	🟨	🟥	🟥	🟥	🟥	🟥	🟩	29,2%
TRACEWRANGLER:	🟥	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟨	🟥	🟥	54,2%

Speed improvements [1]

- Process parallelisation
- GPU Accelerated Crypto
- AES-NI, PadLock, etc.

Image source: www.nvidia.com

Speed improvements [2]

- Special purpose capture cards
  - Programmable NICs and FPGAs
    - Random Number Generator
    - Inline data anonymisation / filtering

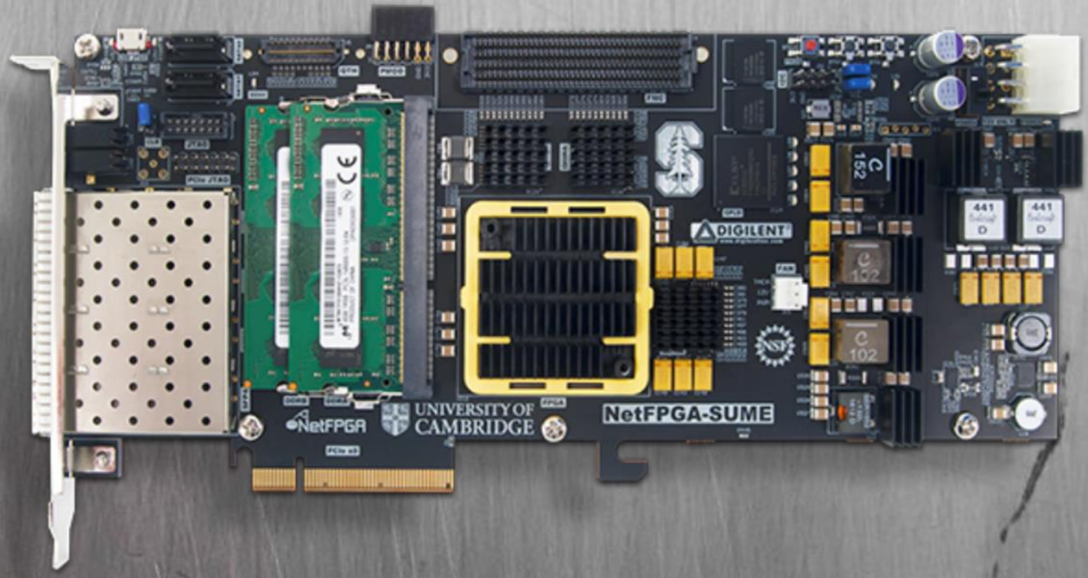


Image source: digilentinc.com/sume/

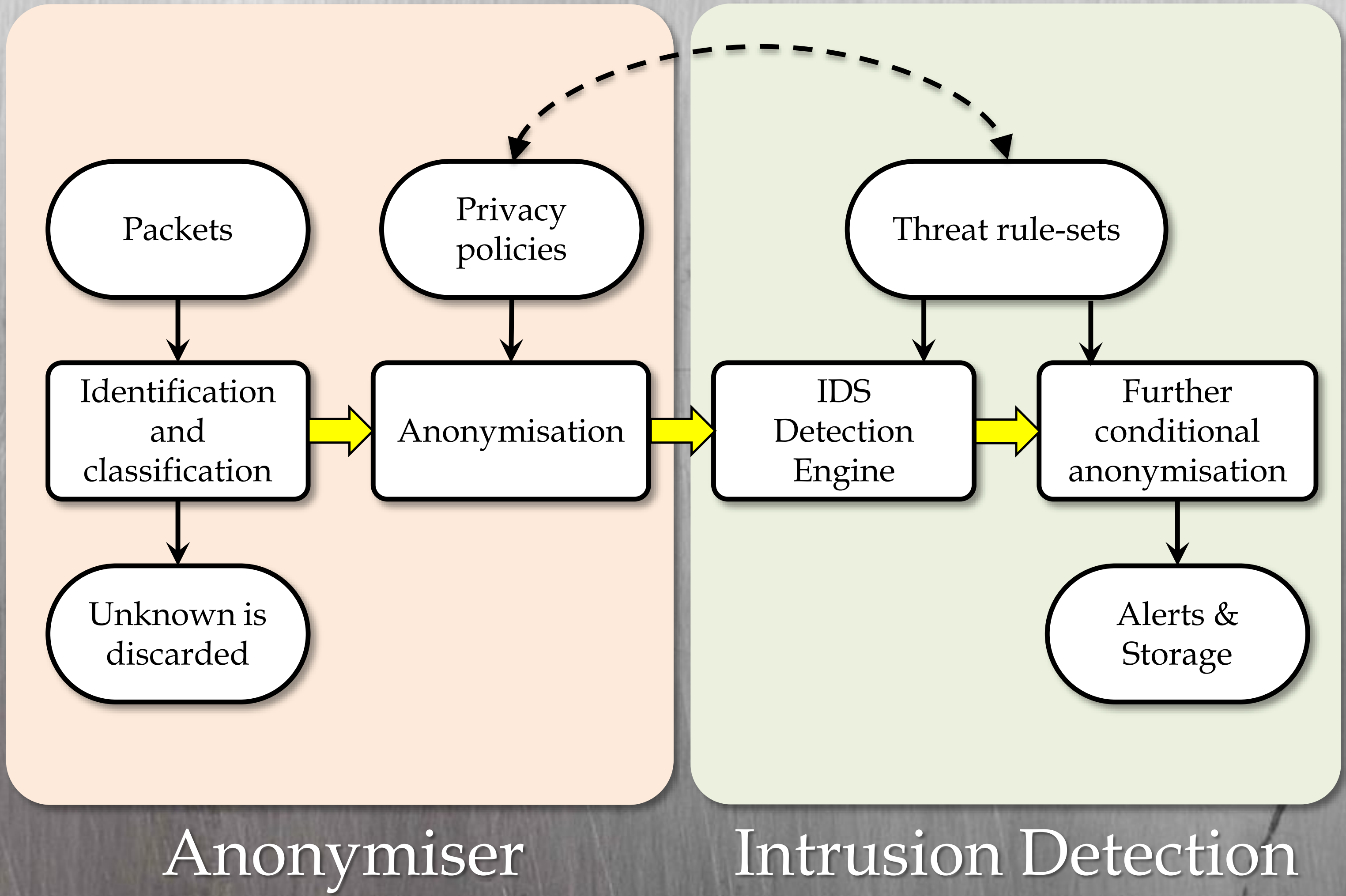
Suggestions

Plan

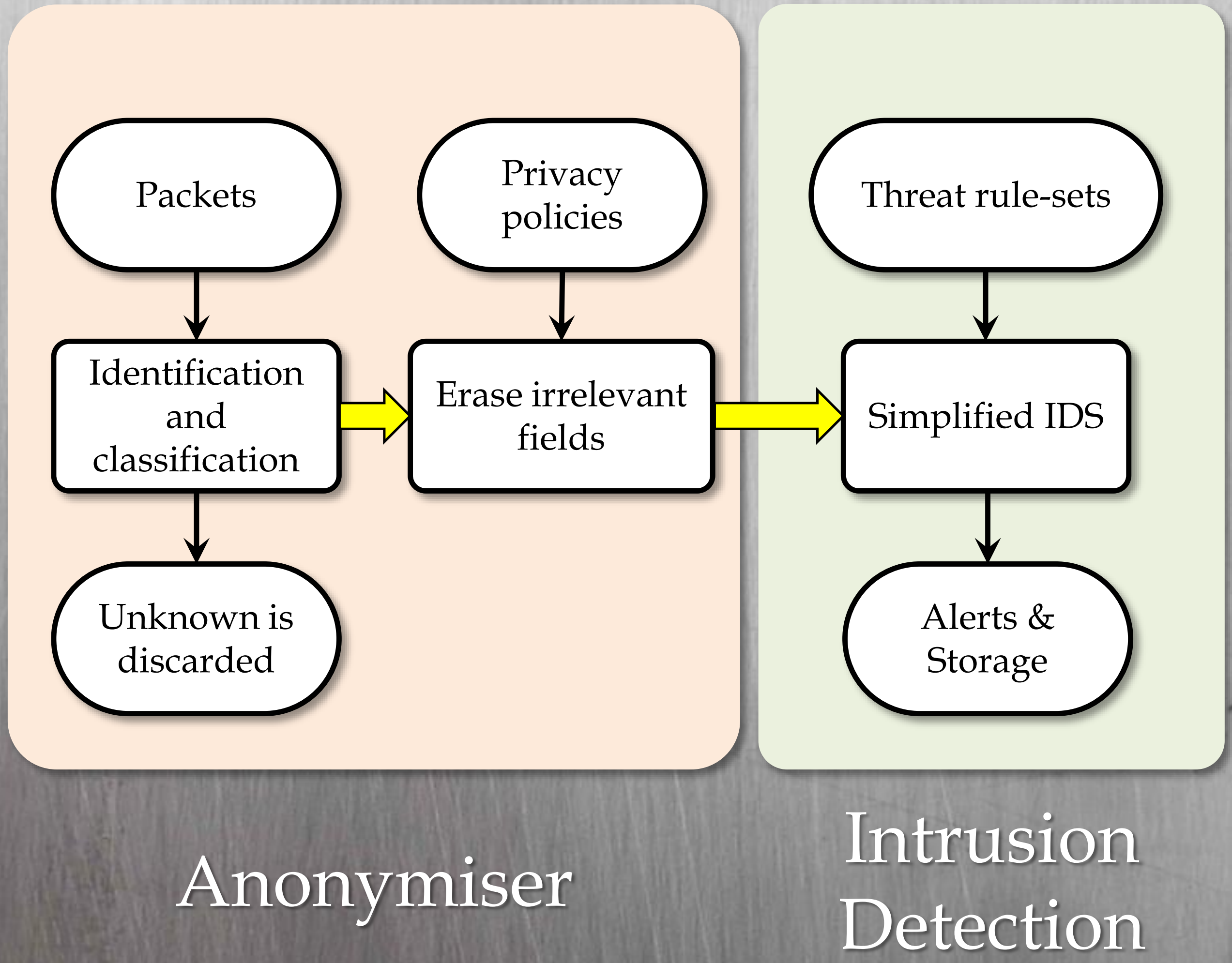
Needed steps:

1. Identify proto/apps;
2. Get statistics;
3. Identify threats;
4. Identify sensitive fields;
5. Build privacy and threat policies.

Network native way



White fielding



Conclusions

Conclusions [1]

It is possible to anonymise network traces to a certain extent and keep some of the usefulness for threat detection

Image source: www.justice-for-families.org.uk/

Conclusions [2]

- Do not share complete datasets;
  - Only specific new threat-related parts;

- Maturity of frameworks:
  - Primitive enhancements;
  - Improving of parsing;
  - Speed / Scalability.

Acknowledgement

Nationaal Cyber Security Centrum

Ministerie van Veiligheid en Justitie