Covert channels and data exfiltration

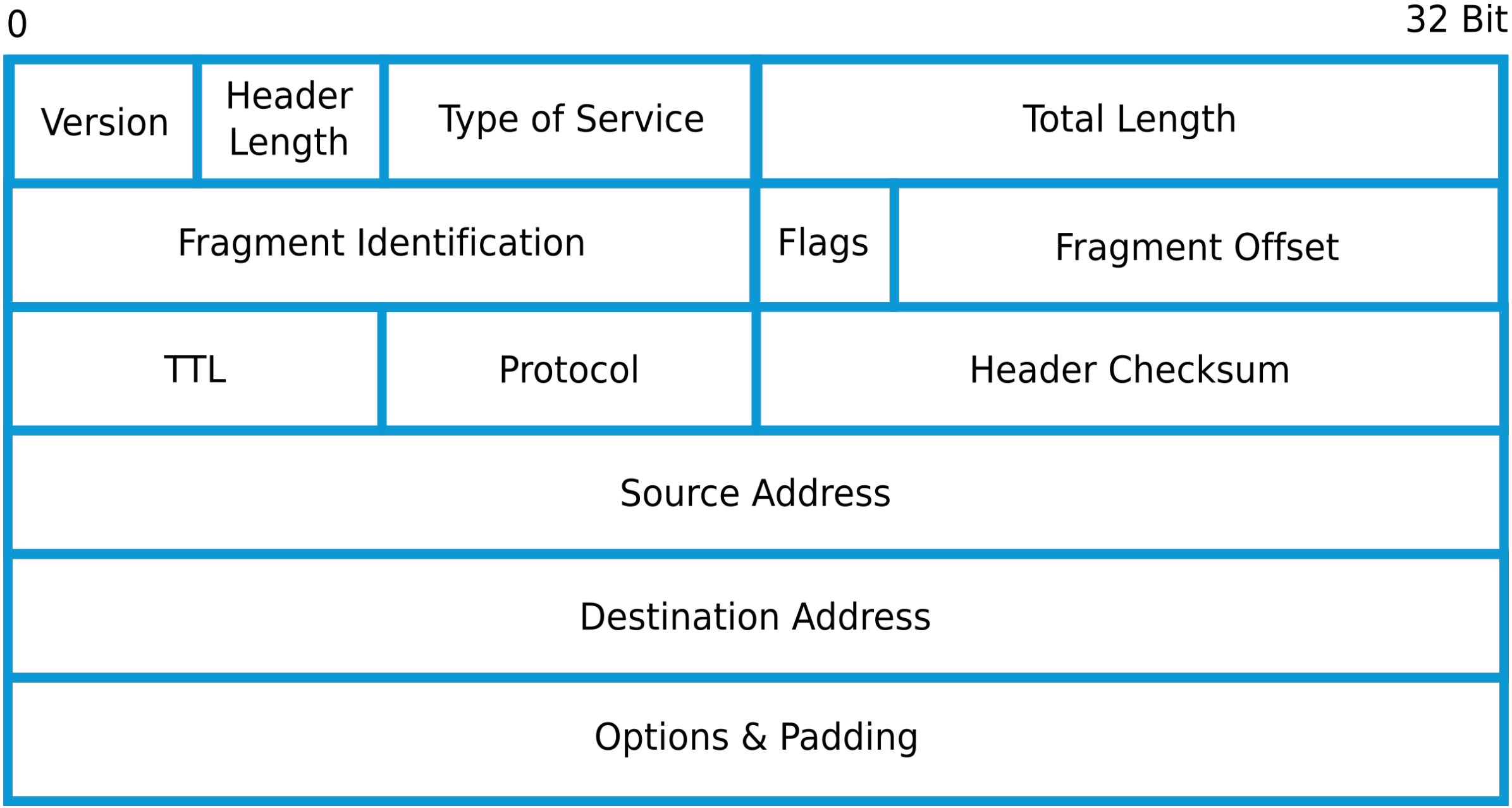
Using a simple covert channel example

- What is a covert channel?
- Covert channel tools and techniques
- Intel AMT Serial over LAN
- Example of homemade covert channel tool
- Covert channel mitigations
- Q&A

Why would we need a covert channel ?

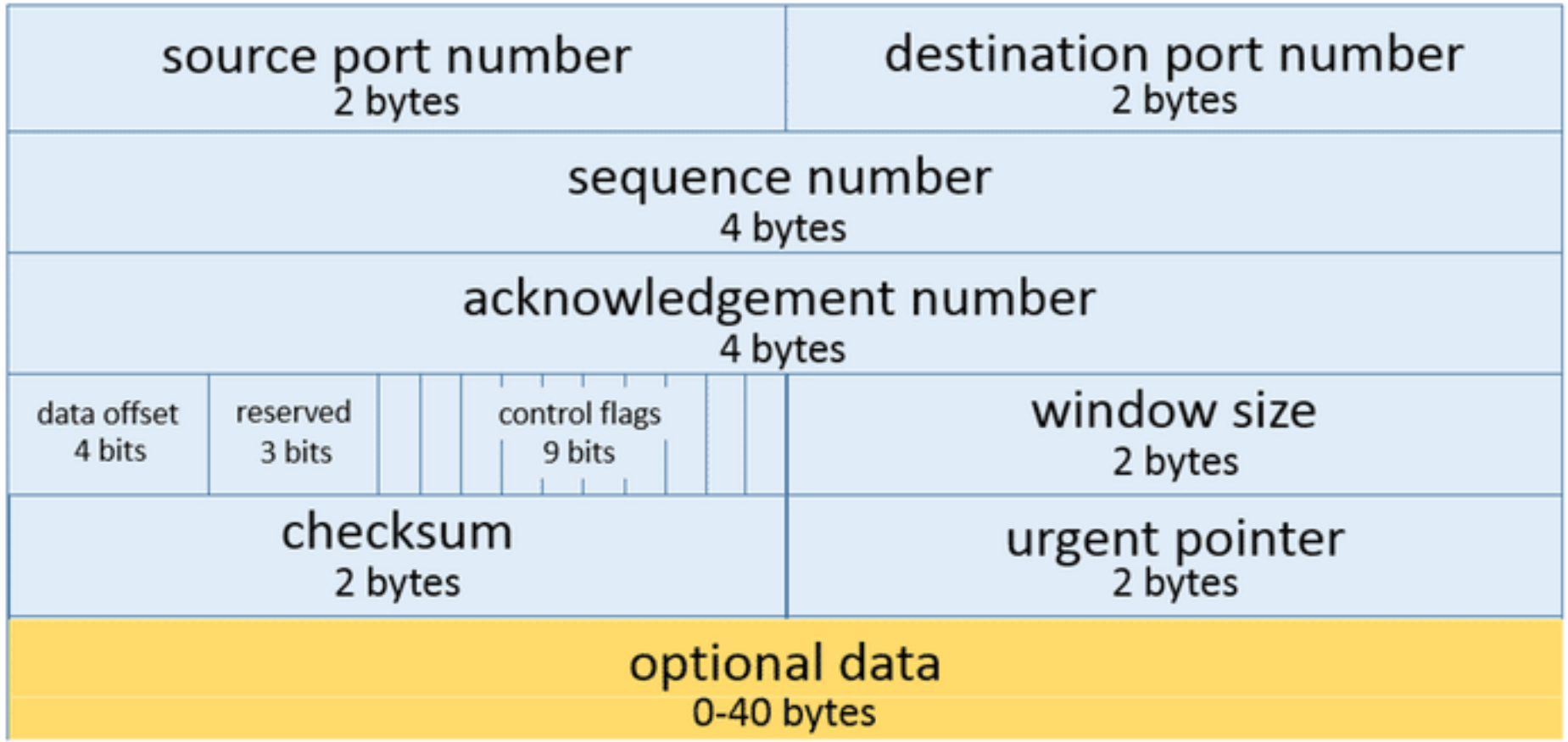
What is a covert channel ?

- Communication channel
- Overt channel
- Covert channel
  - Use existing medium to convey data
  - Bypass access control mechanisms / security policies
  - Misue overt channel properties
- Not considered a covert channel
  - FTP, IRC, File upload service,....


0
32 Bit
Version
Header Length
Type of Service
Total Length
Fragment Identification
Flags
Fragment Offset
TTL
Protocol
Header Checksum
Source Address
Destination Address
Options & Padding

Transmission Control Protocol (TCP) Header

20-60 bytes



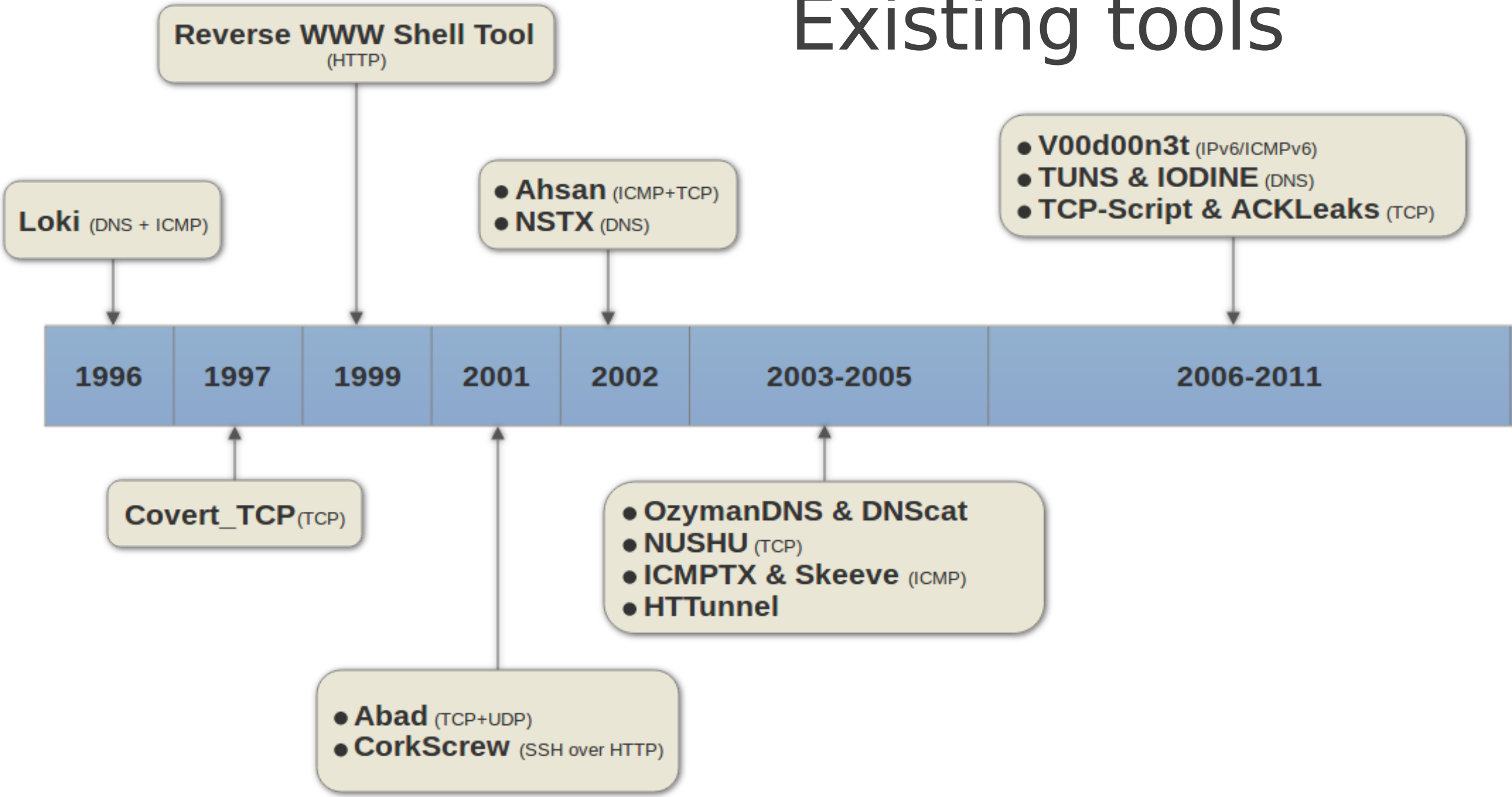
IP Datagram

	Bits 0–7	Bits 8–15	Bits 16–23	Bits 24–31
IP Header (20 bytes)	Version/IHL	Type of service	Length	
	Identification		*flags* and *offset*	
	Time To Live (TTL)	Protocol	Checksum	
	Source IP address			
	Destination IP address			
ICMP Header (8 bytes)	Type of message	Code	Checksum	
	Header Data			
ICMP Payload (*optional*)	Payload Data			

Techniques

- Piggy back on other protocols:
  - TCP/IP → 25+ headers (ToS, Checksum, Fragments size,...)
  - ICMP → payload size or content
  - DNS → within the queries
  - HTTP → Infinite number of headers
  - Virtually any protocol (SIP, RTSP,...)
- Non-networking covert channels:
  - Shared hosts
  - Shared storage
  - Time based covert channel

Existing tools



Limitations of existing tools

- Network
  - Firewall rules, including Deep packet inspection (DPI)
  - Anomaly based network analysis
  - Blacklisted IP or Domain
- Client operating system
  - Antivirus might detect the tool
  - Tool requirements:
    - An external interpreter (Python, Perl,...)
    - Elevated privileges
    - Work only on a specific operating system (GNU/Linux,...)

Workarounds

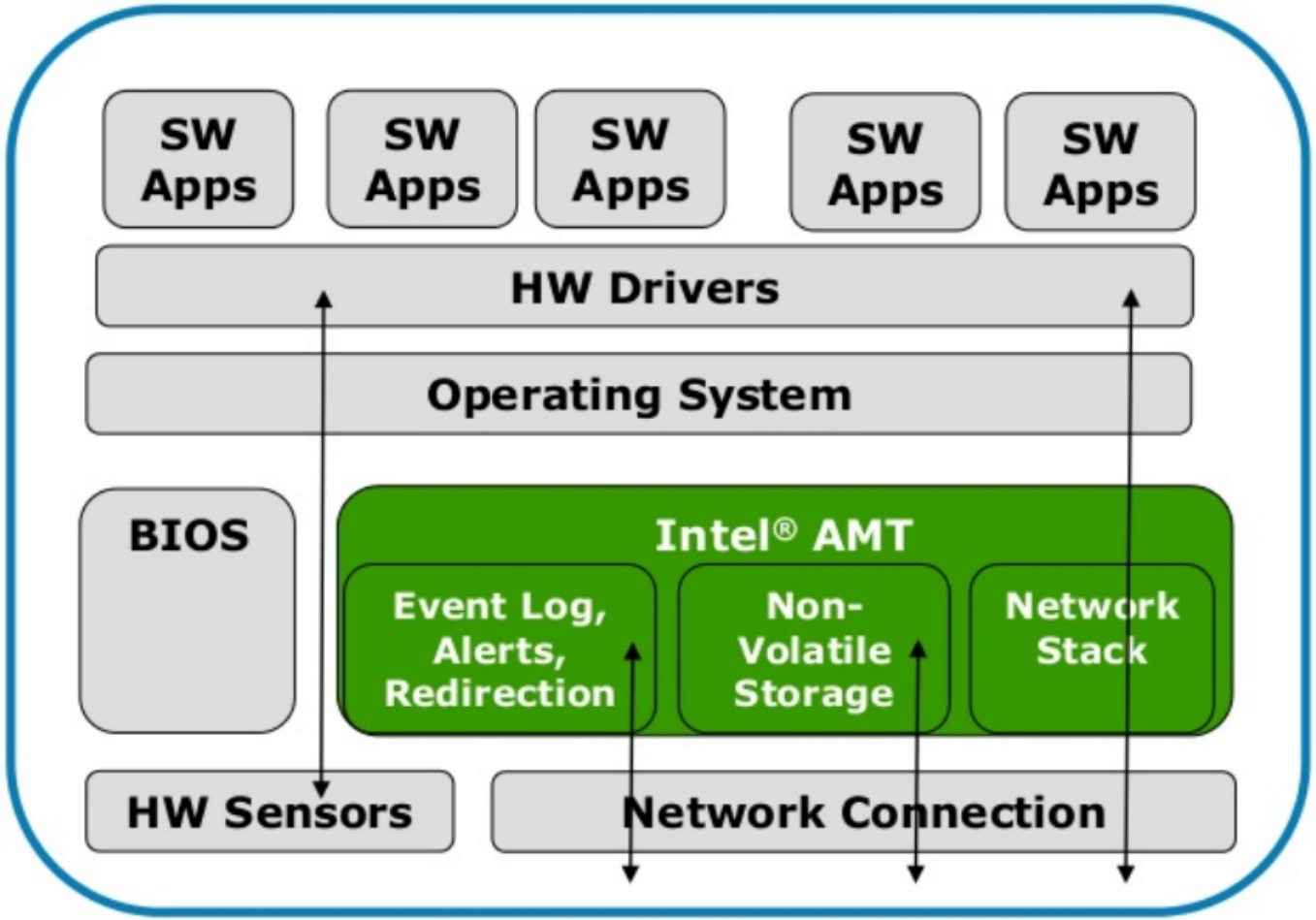
- Network
  - Avoid unusual modification
  - Use IP and Domain with good reputation
  - Keep volume of data transferred low
  - Encrypt
  - Avoid direct communication between client and server
- Client operating system
  - Use tools available out of the box

Intel AMT SoL

- Revealed by Microsoft security research team
- Can be enabled from Operating system
- Independant from the Operating system
  - Communication doesn't go through OS Firewall

Intel® vPro™ Technology

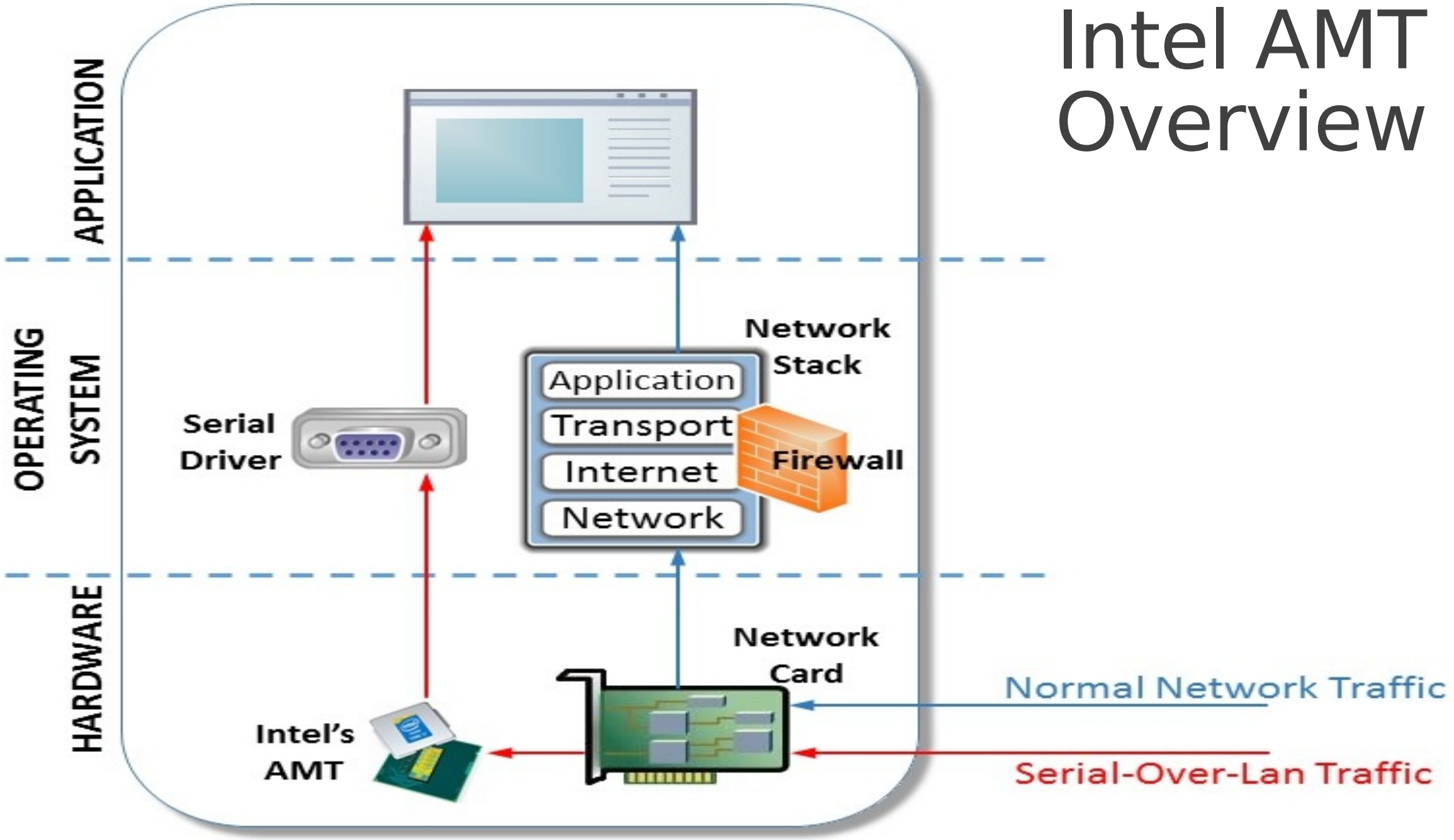
Intel® AMT Architecture



Features
Secure Out Of Band access
Remote troubleshooting and recovery
Proactive alerting
More detailed HW inventory
Third-party, nonvolatile storage

Secure access and control of Intel® vPro™ machines, even OOB

Intel AMT Overview



Example of a simple covert channel tool

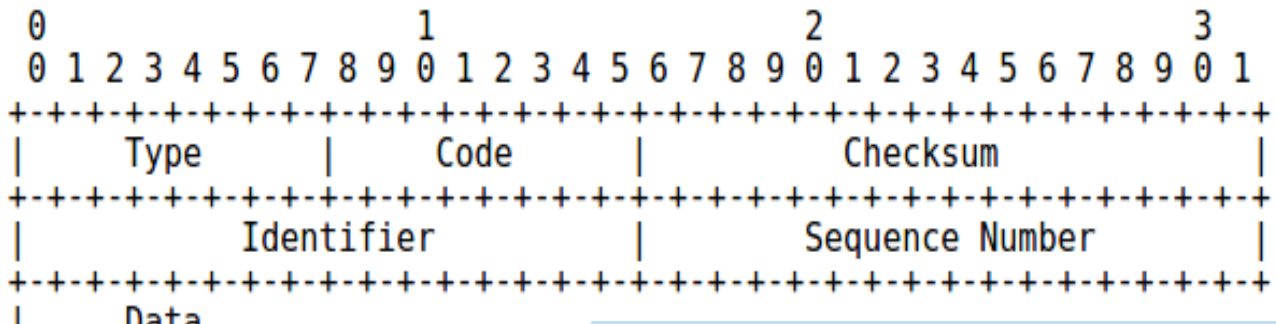
Tool constraints

- Usable on a freshly installed Windows 10 machine
- Impossible to install software
  - Need out of the box tools
- Limited account on the machine (standard user)
  - No admin privileges required

Tool overview

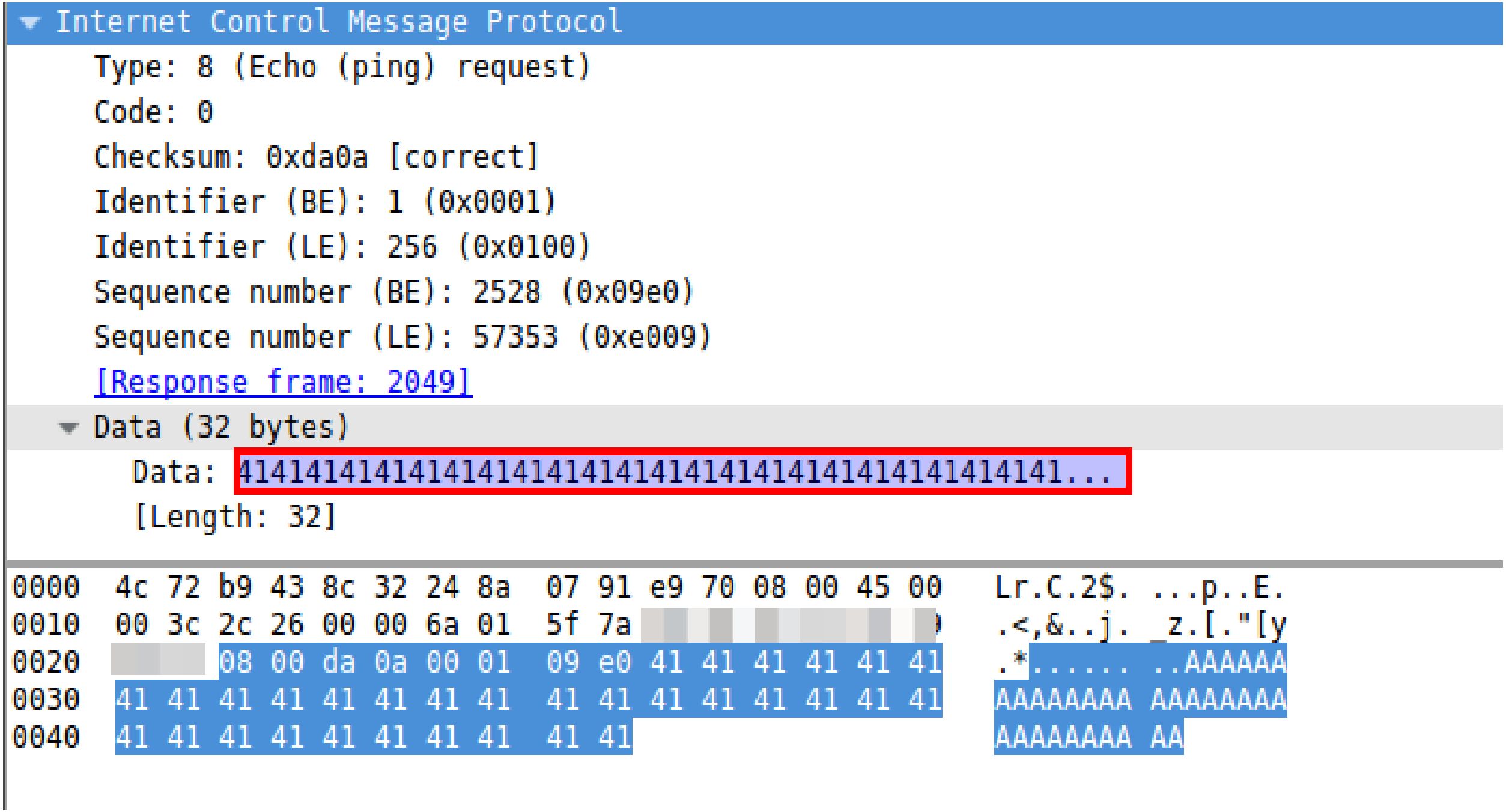
- Use powershell
- Using the ICMP payload to hide our data
- Client
  - Divide our data in 32 Bytes chunks to fit Windows default payload size
  - Send our chunks as ICMP payload
- Server
  - Extract the payload content and print it on screen

Echo or Echo Reply Message




```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d55 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 6 (0x0006)
    Sequence number (LE): 1536 (0x0600)
    [Response frame: 4]
  Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
      [Length: 32]
```

```
0000  02 00 00 00 45 00 00 3c  4d c2 00 00 80 01 00 00   ....E..< M.......
0010  7f 00 00 01 7f 00 00 01  08 00 4d 55 00 01 00 06   ........ ..MU....
0020  61 62 63 64 65 66 67 68  69 6a 6b 6c 6d 6e 6f 70   abcdefgh ijklmnop
0030  71 72 73 74 75 76 77 61  62 63 64 65 66 67 68 69   qrstuvwa bcdefghi
```


Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xda0a [correct]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence number (BE): 2528 (0x09e0)
Sequence number (LE): 57353 (0xe009)
[Response frame: 2049]
Data (32 bytes)
Data: 4141414141414141414141414141414141414141...
[Length: 32]
0000 4c 72 b9 43 8c 32 24 8a 07 91 e9 70 08 00 45 00 Lr.C.2$. ...p..E.
0010 00 3c 2c 26 00 00 6a 01 5f 7a .<,&..j. _z.["[y
0020 08 00 da 0a 00 01 09 e0 41 41 41 41 41 41 .*...... ..AAAAAA
0030 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0040 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AA

Demo: Exfiltrate my file

I want to see the code !

https://github.com/yilmi/pingtransfer

Covert Channels mitigations?

- No Silver bullet
  - Too many techniques and combinations of changes
- Prevention is better than cure
  - DPI/DPL might help for common covert channels
- Have strong security policies and enforce them:
  - Protect against malware attacks
  - Protect valuable assets
  - Have a per need access policy

Q&A