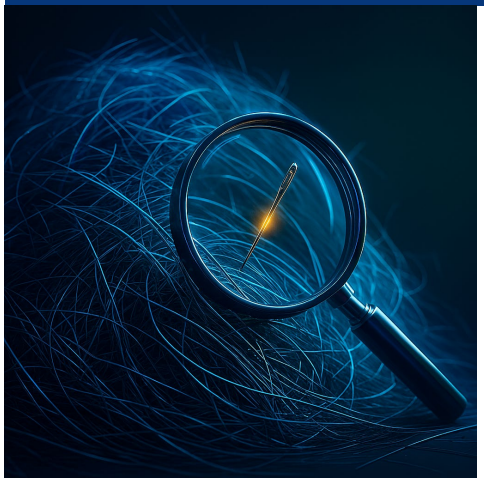
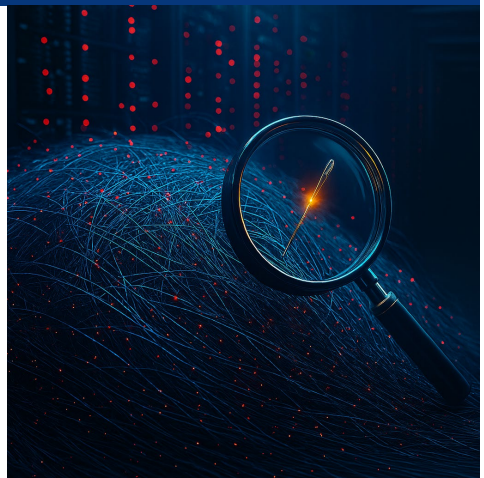
POLIISI
KESKUSRIKOSPOLIISI
Centralkriminalpolisen
National Bureau of Investigation

IP-addresses in criminal Investigation - Finnish view

How to find the Digital needle in digital haystack

Detective Superintendent Ilmari Viro, Head of Telecommunication Unit, National Bureau of Investigation





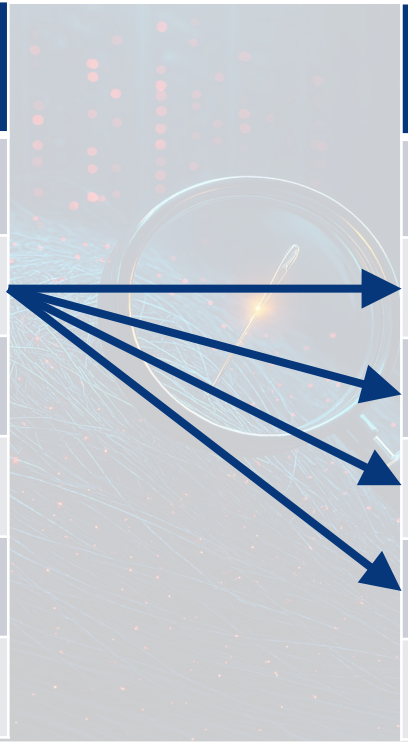
Basis of the Investigation

POLIISI
KESKUSRIKOSPOLIISI
Centralkriminalpolisen
National Bureau of Investigation

The problem in IPv4 without port number

Web service provider records	
Time	IPv4
1	Z
2	J
3	Z
3	L
5	Z

Suspect



ISP/CG-NAT subcriber database			
Time	IPv4	Port	Subcriber
1	Z	A	? Fredrik
1	Z	B	? Joakim
1	Z	C	? Magnus
1	Z	D	? Andreas
3	Z	A	Ilmari

IPv4 port number provided with the query

Suspect

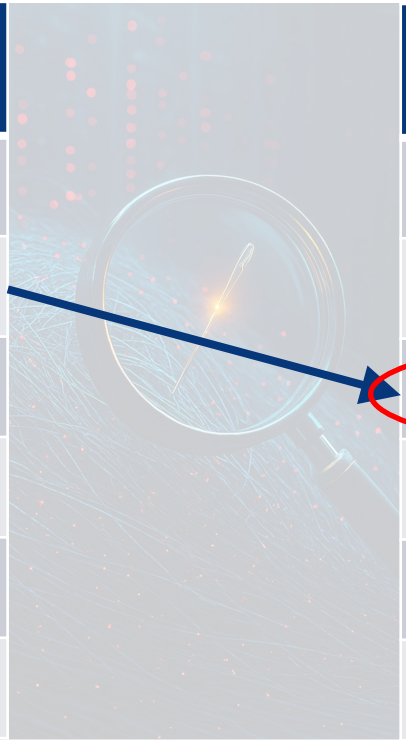
Web service provider records		
Time	IPv4	Port
1	Z	B
2	J	A
3	Z	9
3	L	8
5	Z	7

ISP/CGN subcriber database			
Time	IPv4	Port	Subcriber
1	Z	A	Fredrik
1	Z	B	Joakim
1	Z	C	Magnus
1	Z	D	Andreas
1	Z	1	Ilmari

No problem in IPv6

Suspect

Web service provider records	
Time	IPv6
1	Z:::W
2	J:::N
3	K:::O
3	L:::P
5	M:::R



ISP/CGN subcriber database		
Time	IPv6	Subcriber
1	Z:::X	Fredrik
1	Z:::W	Joakim
1	Z:::Y	Magnus
1	Z:::A	Andreas
1	Z:::1	Ilmari

Year 2012, precautions made

- Back then Finland was evaluating some Data Retention solutions and some reference implementations were seen
- Needle in Haystack – 65536 ports for one IPv4 address – need for better solution
- Meeting with all Mobile network operators in Finland
- Voluntary agreement to limit CG-NAT to absolutely minimum amount of customers behind one public IP
- Growth only step by step 8 (2012)→ 16 → 32 → 64 → 128 → 256 (2025)
- Positive recognition only if investigator can provide timestamp, port and IP – or IPv6 address

POLIISI
KESKUSRIKOSPOLIISI
Centralkriminalpolisen
National Bureau of Investigation

Situation today (in Finland)

- All mobile network operators will assign IPv6 addresses
- Most public web services run also in IPv6
- All small or shady services and still run on IPv4 – need for operators to assign also IPv4 addresses
- Not all Service providers are saving port information in IPv4 services – how to enforce – DR does not apply to web services.
- Is there technical barriers to prevent CG-NAT in IPv6?
- **Indicator exists – if MNO's manage to limit reserved IPv4 allocation down from current 256 customers → then we know that IPv6 is gaining momentum → at least within our "customers".**

Anonymity vs. Lawful Access

- When adopting security BigTech and others utilizes E2EE
  - Security and responsibilities shifted to the User
  - No moderation needed
  - No need for Lawful Access team
  - Only limited access for metadata including location – growing importance for LEA's.
  - Protection of privacy is lifted from criminals by access warrant
  - Need for transparent, accountable and secure lawful access solutions
  - Technical solutions: It would be possible to target individual suspect – willingness is missing – cost of change
  - No regulation was choise to promote innovation in early days of internet – now there is need for regulation – or it will be only the playground for the strongest
  - Law Enforcement Operational Needs LEON-document

Tack