Politiet bruger logning af telefonitrafik i forbindelse med efterforskning og retsforfølgning

For at følge med udviklingen har politiet brug for tilsvarende logning af internettrafik

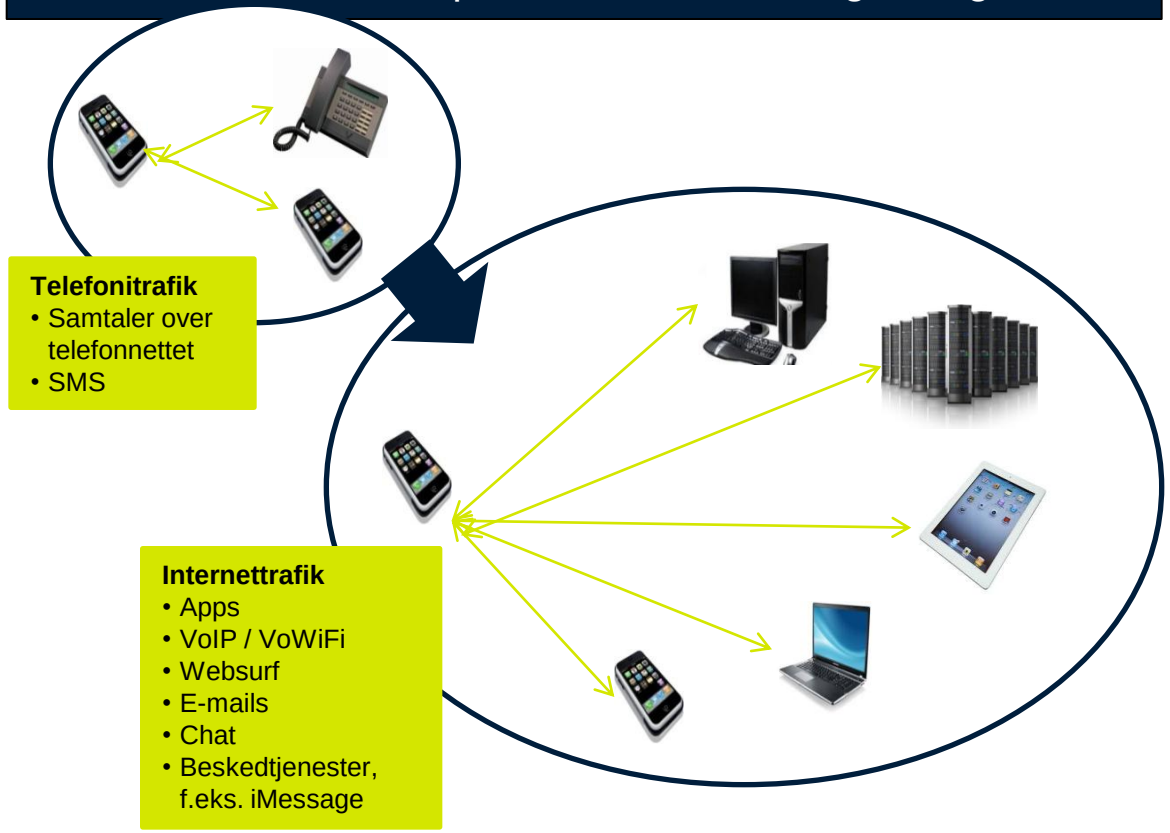
22. FEBRUAR 2016

To udviklingstendenser skærper politiets behov for adgang til digitale spor og dermed logning af internettrafik

Kriminaliteten flytter fra den fysiske verden til internettet. It-kriminalitet og økonomisk kriminalitet via nettet stiger, mens den generelle kriminalitet falder.

- Der finder stort set ikke længere bankrøverier sted – i dag lænses pengeinstitutter via nettet.
- Hackerangreb bestilles via nettet for få midler - kriminalitet er blevet en service, man kan bestille over nettet
- Oplysninger om betalingskort købes via nettet til brug for økonomisk kriminalitet.
- Anmeldelser relateret til online handel er tredoblet fra 2009 til 2014.

Kommunikation foregår i stigende grad via internettet. Derfor er der behov for også at logge oplysninger om internettrafik – ellers udhules politiets efterforskningsmuligheder.



POLITI

Hvad er logning?

- Logning er registrering og opbevaring af oplysninger om tele- og internet***trafik***. Dvs. oplysninger om kommunikationsspor:
  - Hvem kommunikerede med hvem?
  - Hvor og hvornår fandt denne kommunikation sted?
  - Hvilket udstyr, blev der anvendt i forbindelse med kommunikationen?

- Logningen indeholder *ikke* oplysninger om selve kommunikations***indholdet*** (herunder URL) - hverken i forbindelse med telefonsamtaler eller ved brug af internettet.

- Politiets brug af loggede oplysninger forudsætter rettens kendelse

Eksempel på loggede oplysninger:

Afsender IP	Modtager IP	Transport -protokol	Afsendende Portnummer	Modtagende Portnummer	Volumen (bytes)	Tidspunkt start	Tidspunkt slut
6.6.6.6	1.2.3.4	TCP	13423	22	2003232	7/5-2016, 12:24:23.433	7/5-20 12:54:51.2
1.2.3.4	5.6.7.8	TCP	63423	80	1924823	7/5-2016, 12:25:23.823	7/5-2016, 12:54:37.251
6.6.6.6	1.2.3.4	TCP	3431	22	4883290	9/5-2016, 15:34:38.329	9/5-2016, 16:27:23.834

Logning omfatter *ikke* indhold - eksempelvis:

113:45: Post på Facebook: ”xx fortjener nogle tørre tæsk”
114:04: Like på Facebook: ”Fri hash i Danmark”
114:08: Indkøbskurvens indhold på Apotek.dk
114:15: Mail fra g-mail til vens mailadresse

POLITI

Logning kan styrke indsatsen mod

Politiet har i mange år i vidt omfang brugt loggede oplysninger om telefonitrafik i forbindelse med **efterforskning** og **retsforfølgning** af kriminalitet. På grund af udviklingen har politiet et stigende behov for også at kunne anvende digitale spor i efterforskningen af:

- Kriminalitet, der retter sig imod it-systemer, fx hacking
- Kriminalitet, der begås under anvendelse af it, fx netbank-indbrud eller online seksuelt misbrug af børn
- Alle former for kriminalitet, hvor digitale spor kan indgå som bevis, fx terrorisme, menneskesmugling, drab og narko

POLITI

Politiet ønsker logning af internettrafik svarende til den logning af telefontrafik, der allerede foregår i dag.

Logning af telefonitrafik (sker allerede i dag)

- Hvilke telefonnumre har været sat i forbindelse med hinanden
- Kommunikationens starttidspunkt
- kommunikationens sluttidspunkt
- Varighed af samtale

Særligt for mobiltelefoni:

- Hvilket udstyr har været brugt ved kommunikationen (IMEI, IMSI)
- Hvilket mobilmaster har været brugt i forbindelse med kommunikationen

Logning af internettrafik (Det politiet ønsker)

- Hvilke IP-adresser har været sat i forbindelse med hinanden
- Hvilken transportprotokol og hvilke portnumre har været anvendt
- Kommunikationens starttidspunkt
- Kommunikationens sluttidspunkt
- Antal bytes der er overført

Særligt for ikke-kablet internet:

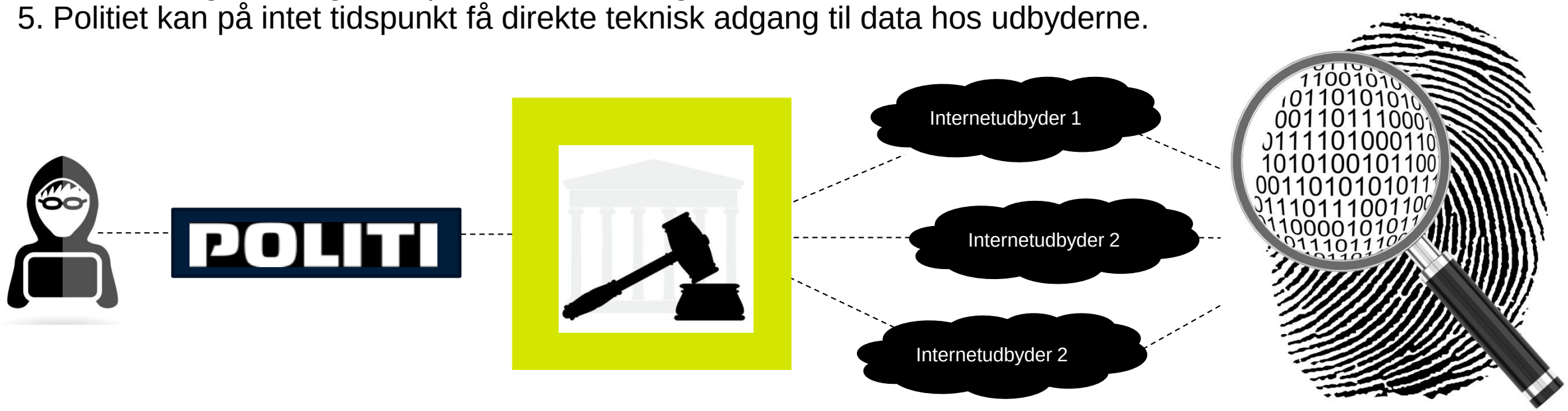
- Hvilket udstyr har været brugt ved kommunikationen (IMEI, IMSI)
- Hvilket mobilmaster har været brugt i forbindelse med kommunikationen

Grundlæggende er der tale om **samme type** af oplysninger,
Logning af telefonitrafik **adskiller sig teknisk** fra logning af internettrafik

POLITI

Politiets brug af loggede oplysninger kræver en dommerkendelse

1. Kriminalitet begås
2. Politiet har brug for digitale spor og indhenter dommerkendelse
3. Internetudbydere udleverer loggede trafik-oplysninger til politiet
4. Politiet bruger de digitale spor i efterforskningen
5. Politiet kan på intet tidspunkt få direkte teknisk adgang til data hos udbyderne.

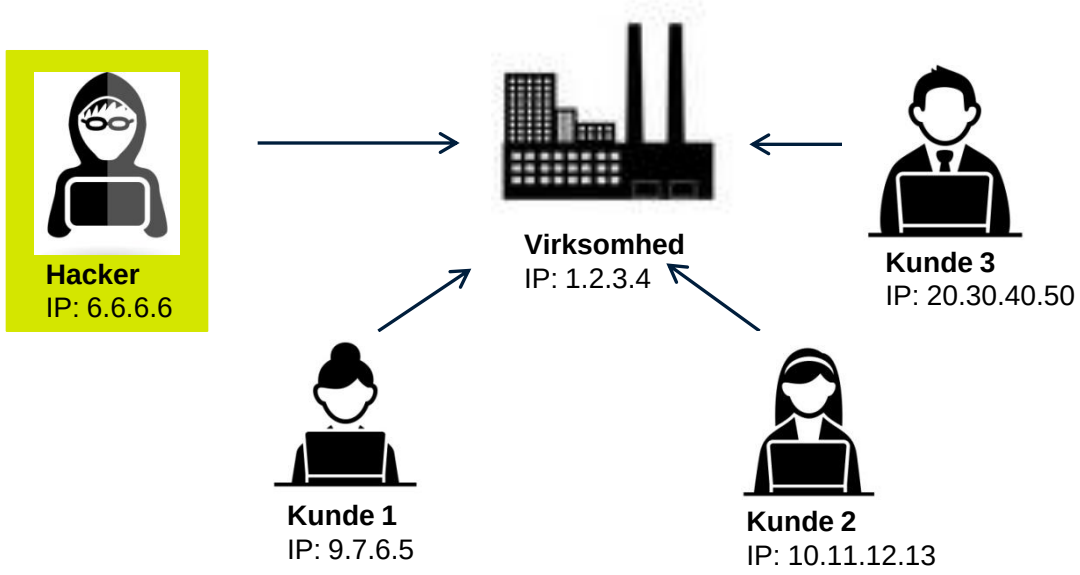


Eksempel 1: Virksomhed hackes

Virksomhed opdager, at den er blevet hacket og tager kontakt til politiet, der vurderer, at efterforskningen har brug for digitale spor. Dommerkendelse indhentes og loggede oplysninger udleveres af internetudbyderen.

Den rekvirerede logning skaber indblik i, hvilke IP-adresser der har været i kontakt med den hackede virksomhed i det relevante tidsinterval.

Næste skridt vil være at se på, hvem der er relevant at efterforske ud fra den adfærd, logningen peger på, i kombination med andre efterforskningsspor.



LOGNING FRA INTERNETUDBYDEREN

Afsender IP	Modtager IP	Transport-protokol	Afsendende Portnummer	Modtagende Portnummer	Volumen (bytes)	Tidspunkt start	Tidspunkt slut
9.7.6.5	1.2.3.4	TCP	13423	80	134324	9/12-2016, 13:34:12.323	9/12-2016, 13:43:23.439
10.11.12.13	1.2.3.4	TCP	63423	80	852994	9/12-2016, 14:23:16.895	9/12-2016, 14:32:51.954
6.6.6.6	1.2.3.4	TCP	4323	80	10233239	9/12-2016, 15:23:53.322	9/12-2016, 15:34:18.434
20.30.40.50	1.2.3.4	TCP	4832	80	314123	9/12-2016, 17:48:12.854	9/12-2016, 18:01:32.853

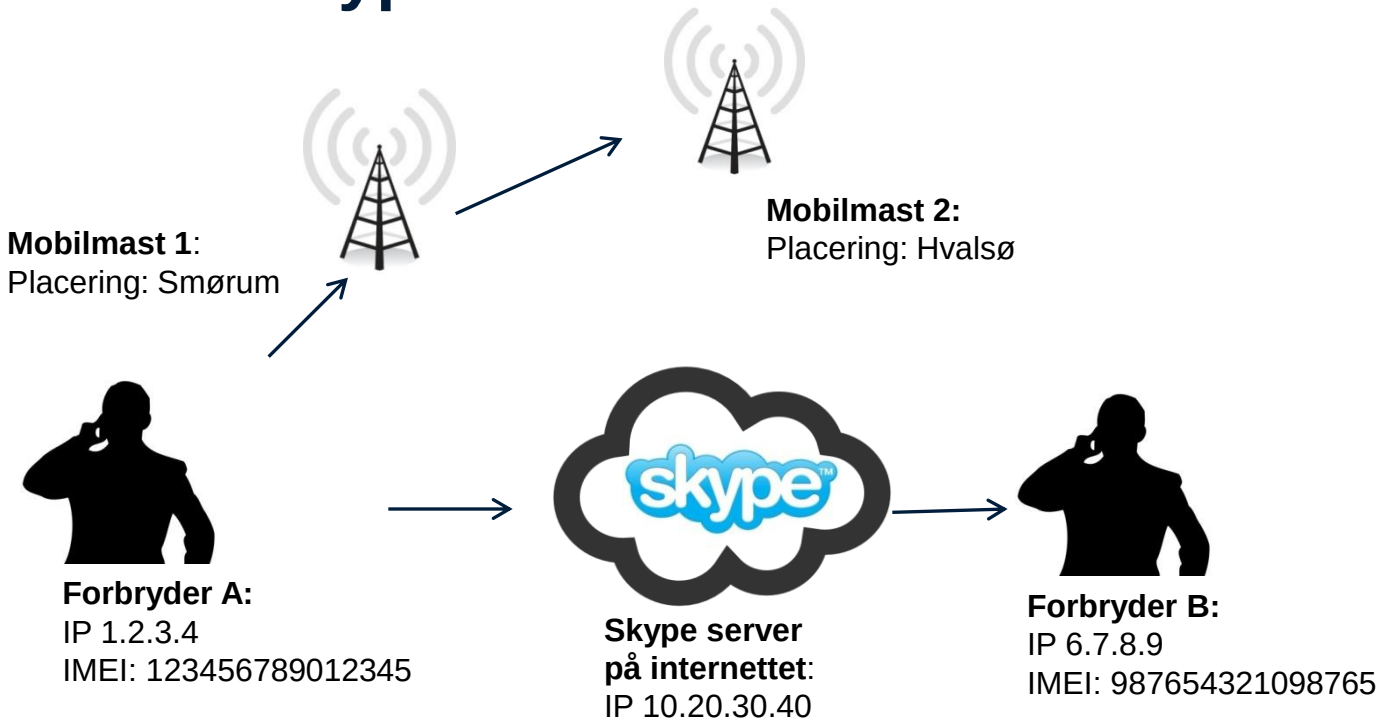
Hacker

POLITI

Eksempel 2:
Forbrydere med mobiltelefoner med Skype

Lgning af internetoplysninger kan afsløre, hvem der kommunikerer med hvem via internettet (ex. Skype. WhatsApp og FaceTime). Teknisk set ringer forbryder A til Skype og forbindes med forbryder B. Efter kort tid foregår kommunikationen direkte mellem forbryder A og B, og dermed kan forbryder B i mange tilfælde identificeres/lokaliseres.

Hvis kommunikationen foregår på mobil-telefoner, kan forbrydernes omtrentlige placering lokaliseres via mobilmaster.
I dette tilfælde afslører masteoplysninger, at forbryder A først er i Smørum, men bevæ-ger sig til Hvalsø.



LOGNING FRA INTERNETUDBYDEREN

Afsender IP	Modtager IP	Transport-protokol	Afsendende Portnummer	Modtagende Portnummer	Volumen (bytes)	Tidspunkt start	Tidspunkt slut	Mobilmast start, Placering	Mobilmast start, celle	Mobilmast slut, placering	Mobilmast slut, celle	IMEI
1.2.3.4	10.20.30.40	UDP	13423	3478	100332	2/4-2016, 3:24:12.013	2/4-2016, 3:25:01.432	Hvalsø	220	Hvalsø	220	123456789012345
1.2.3.4	6.7.8.9	UDP	63423	61234	10232832	2/4-2016, 3:24:56.196	2/4-2016, 3:40:19.734	Hvalsø	220	Tølløse	45	123456789012345

Forbryder A **Skype-server på internettet** **Forbryder B**

POLITI

Eksempel 3:
Logning er også et redskab til at beskytte uskyldige borgere

Virksomhed hackes og anmelder det til politiet. Borgeren, hvis computer indbruddet er begået fra, er uskyldig.

Politiet indhenter dommerkendelse og får logning i relevant tidsrum udleveret.

De loggede oplysninger giver en stærk formodning om, at det ikke er borgeren, der har lavet indbruddet, og sporene peger på en anden gerningsmand.

Uden logning af internetoplysninger kan politiet ikke nødvendigvis se, om borgerens computer har været fjernstyret. Logning får dermed også en beskyttende funktion.

Hacker
IP: 6.6.6.6

Uskyldig borger
IP: 1.2.3.4

Virksomhed
IP: 5.6.7.8

LOGNING FRA INTERNETUDBYDEREN

Afsender IP	Modtager IP	Transport-protokol	Afsendende Portnummer	Modtagende Portnummer	Volumen (bytes)	Tidspunkt start	Tidspunkt slut
6.6.6.6	1.2.3.4	TCP	13423	22	2003232	7/5-2016, 12:24:23.433	7/5-2016, 12:54:51.231
1.2.3.4	5.6.7.8	TCP	63423	80	1924823	7/5-2016, 12:25:23.823	7/5-2016, 12:54:37.251
6.6.6.6	1.2.3.4	TCP	3431	22	4883290	9/5-2016, 15:34:38.329	9/5-2016, 16:27:23.834
1.2.3.4	5.6.7.8	TCP	7532	80	4506433	9/5-2016, 15:35:12.934	9/5-2016, 16:24:45.984

Hacker

Uskyldig borger

POLITI