

[Protokollbilaga D.2 – bilaga till IT-forensiskt undersökningsprotokoll]

[Grovt spioneri alt. grov obehörig befattningsmed hemlig uppgift]

Säkerhetspolisen

Datum: [2022-10-31]

Diarienummer: [0105-K004-17]

Titel: [Protokollbilaga D.2 – bilaga till IT-forensiskt undersökningsprotokoll]

Innehållsförteckning

1.1	Analys av återskapade foton från B063-21-24	1
1.2	Angående spår i Lenovo-datorn och Säkerhetspolisens utskriftsloggar.....	9
1.3	Angående Peyman KIA:s tillgång till Excel-filen [REDACTED].xls' enligt Säkerhetspolisens datasystem	13
1.4	Beskrivning av [REDACTED], Säkerhetspolisen.....	28

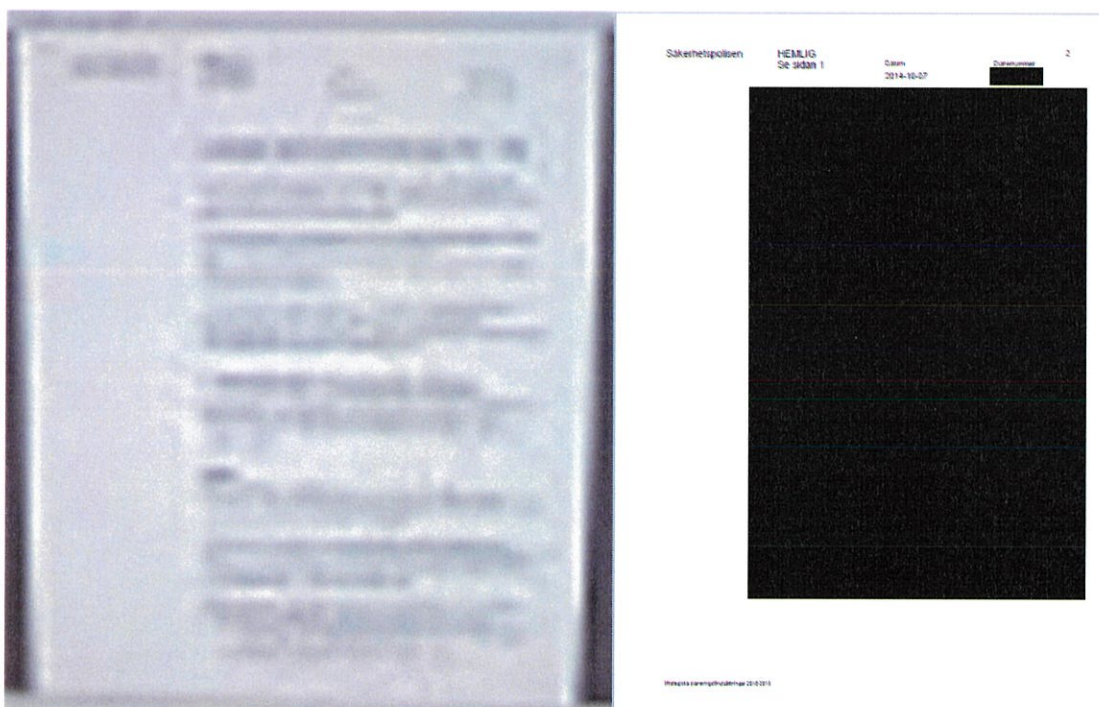
Datum: 2022-02-15
Diarienummer: 0105-K004-17
Namn: [REDACTED]
Titel: Operativ handläggare

[Analys av återskapade foton från B063-21-24]

Inom ramen för förundersökning K004-17 i vilken Peyman KIA [REDACTED] och Payam KIA [REDACTED] är misstänkta för grovt spioneri, genomfördes husrannsakan hemma hos Peyman på Hörnovägen 2, Uppsala. I bostaden beslagtogs en laptop av märket Lenovo (B063-21-24). Från laptopen kunde 39 bilder återskapas. De flesta bilder är fotografier av datorskrmar. 22 bilder är fotografier av vad som ser ut att vara en tabell i Excel eller motsvarande. Tre bilder är fotografier av vad som ser ut att vara ett utskrivet papper. En bild ser ut att vara fotografi av en kalender i Outlook eller motsvarande. 13 bilder är fotografier av vad som ser ut att vara sidor i en rapport, med text och diagram. Bilderna har redigerats för bättre upplösning. I detta dokument har endast delen som motsvarar det avbildade dokumentet klippts in.

Jämförelse

13 av bilderna motsvarar sidor från den 15 sidor långa hemligstämplade rapporten [REDACTED]. De 13 bilderna ligger i samma ordning som i den ursprungliga rapporten. Endast försättsbladet och den sista sidan saknas bland de återskapade bilderna.

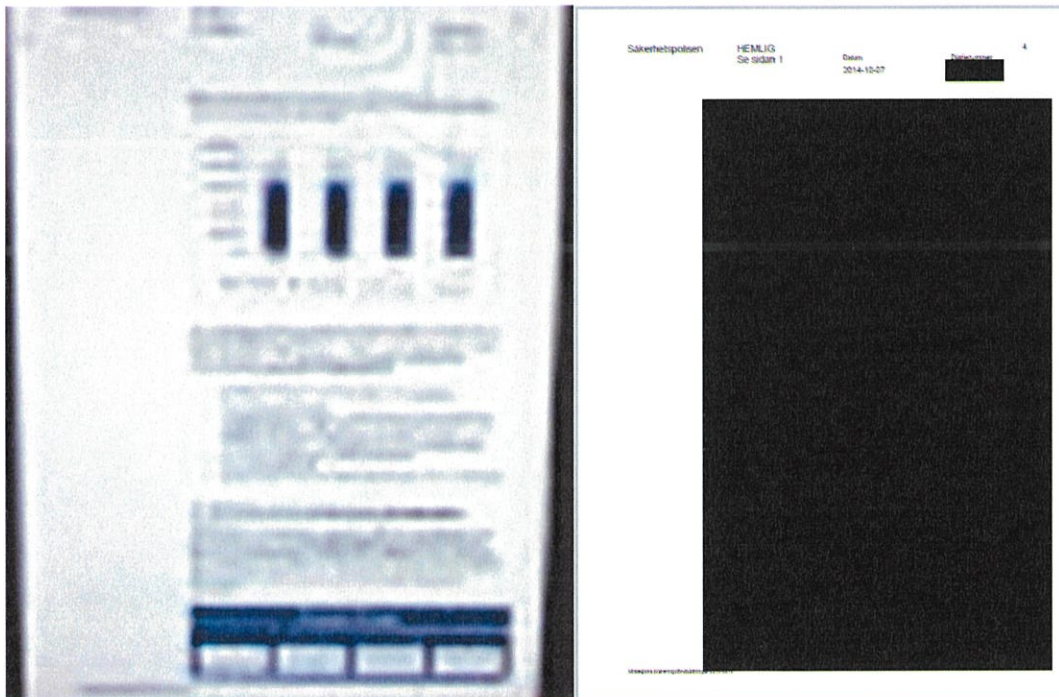
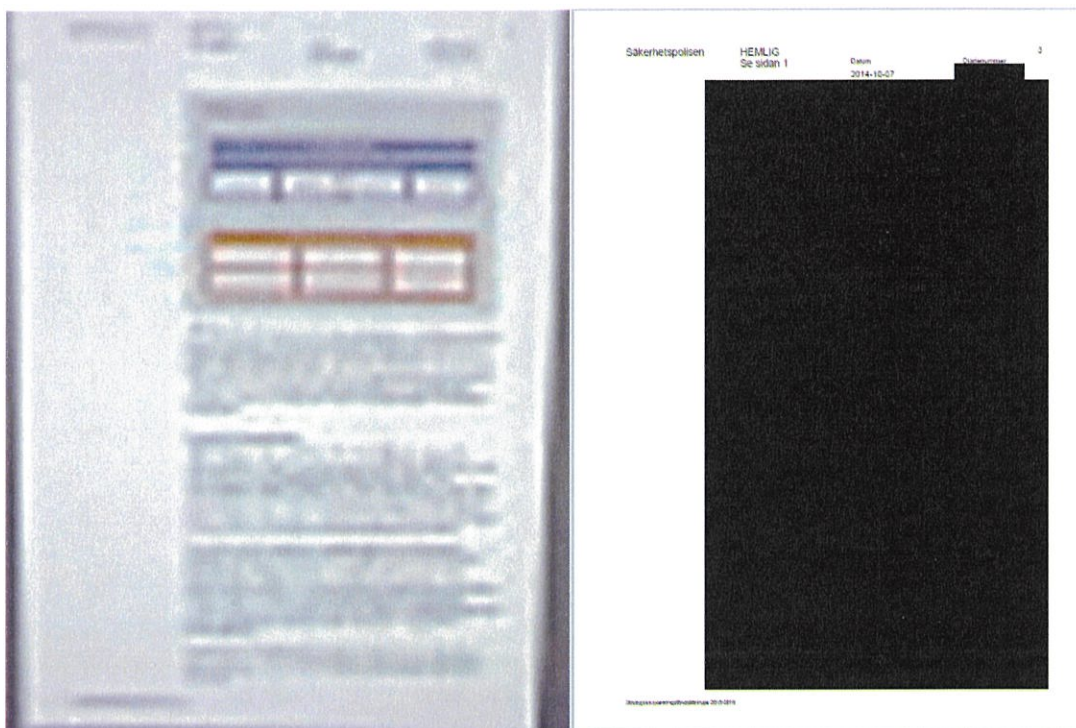


Säkerhetspolisen

Datum: 2022-02-15

Diarienummer: 0105-K004-17

2(8)

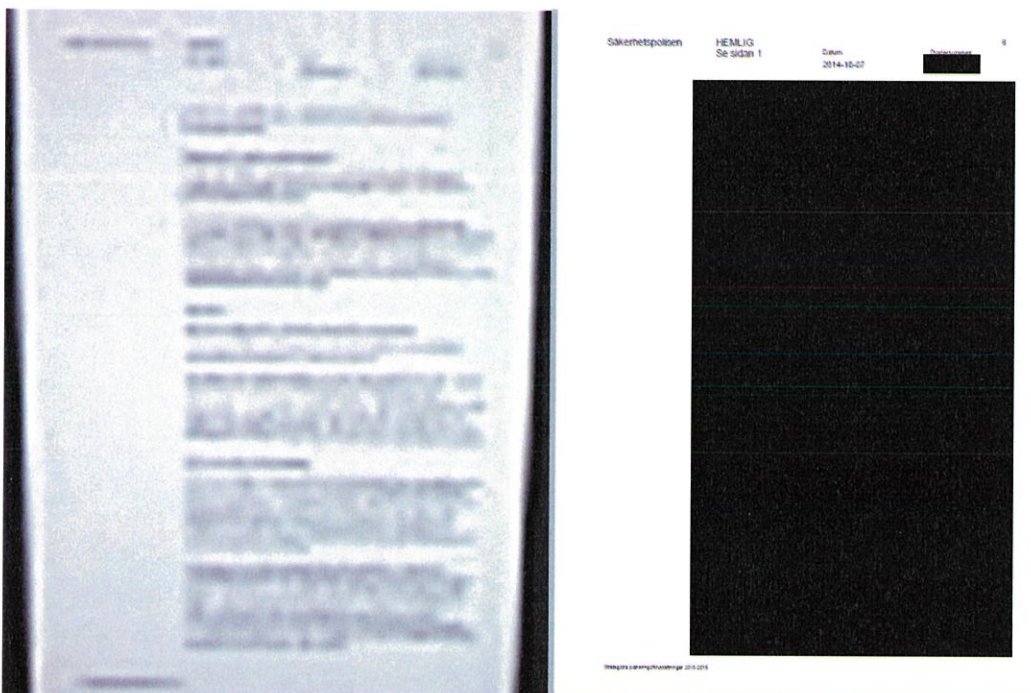
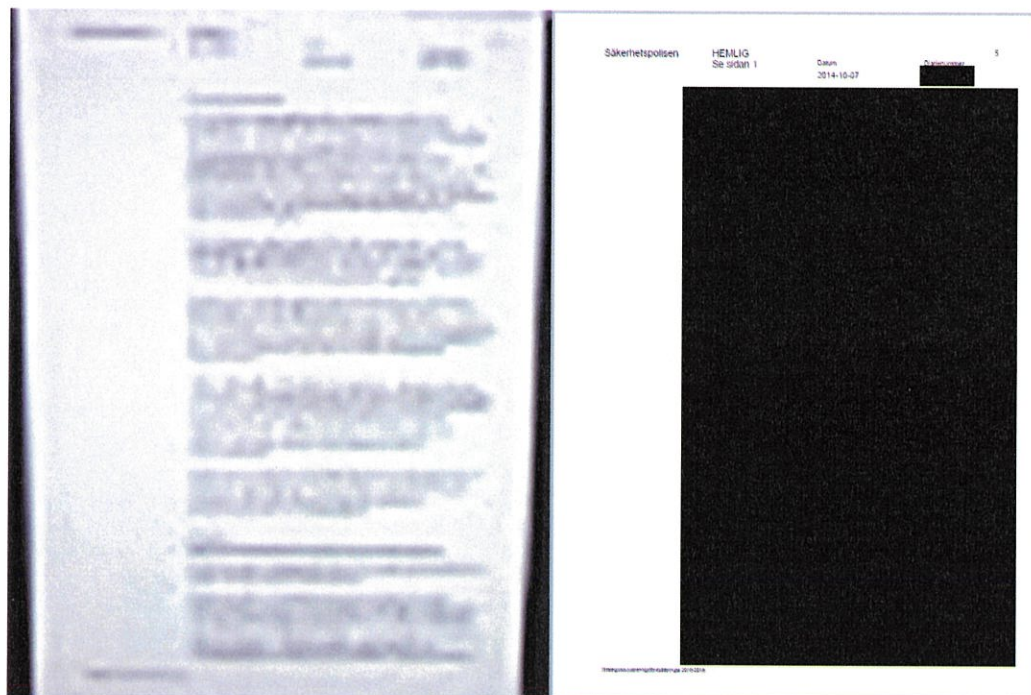


Säkerhetspolisen

Datum: 2022-02-15

Diarienummer: 0105-K004-17

3(8)

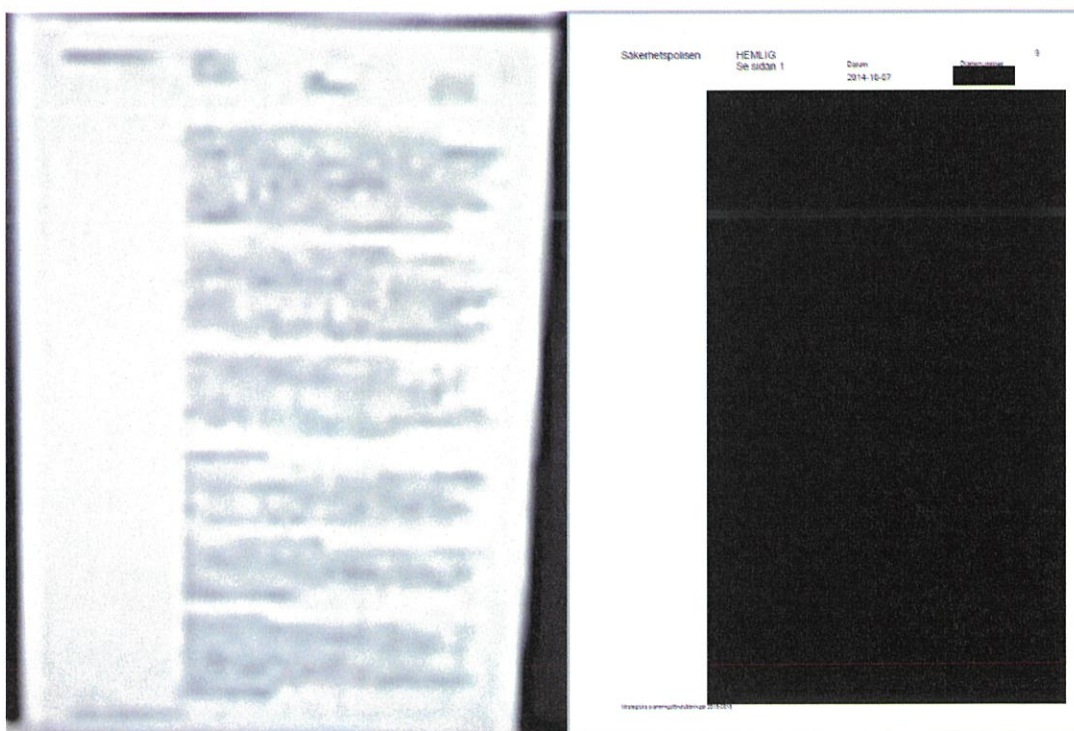
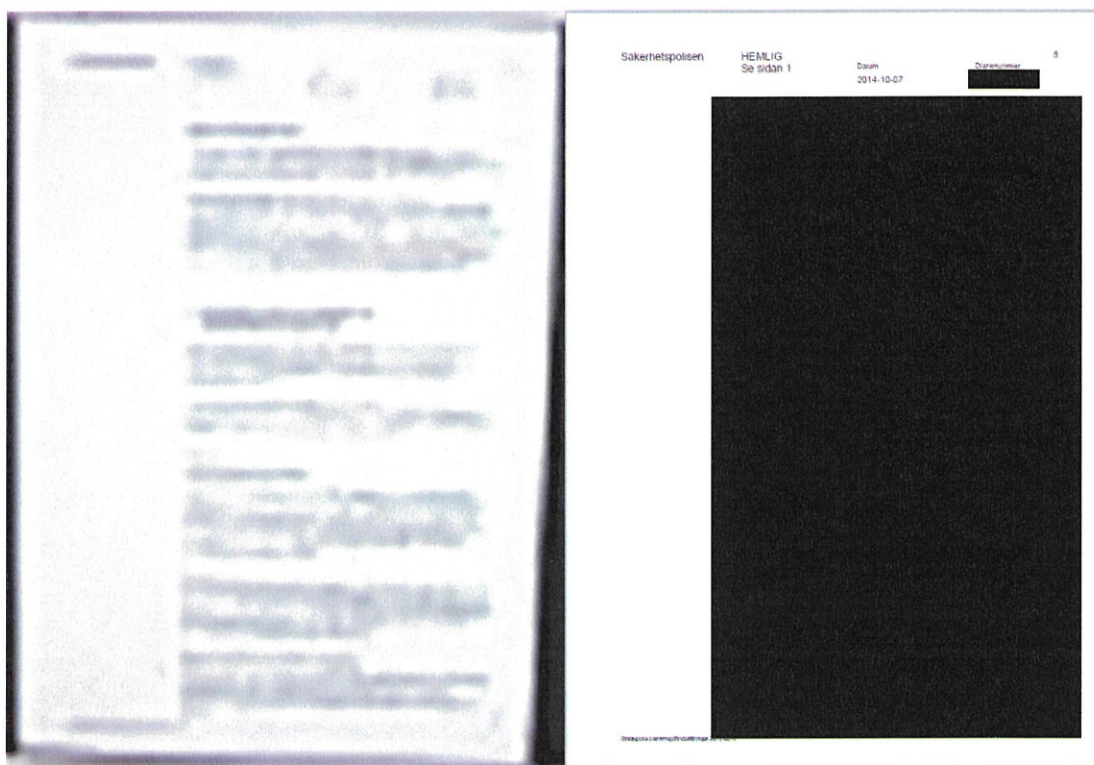


Säkerhetspolisen

Datum: 2022-02-15

Diarienummer: 0105-K004-17

4(8)

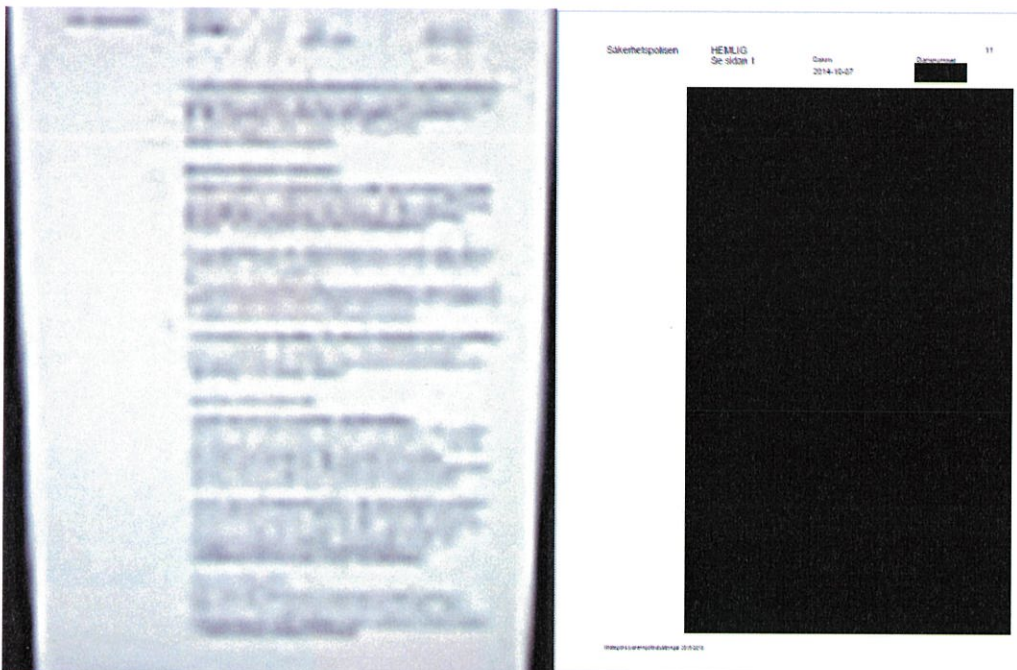
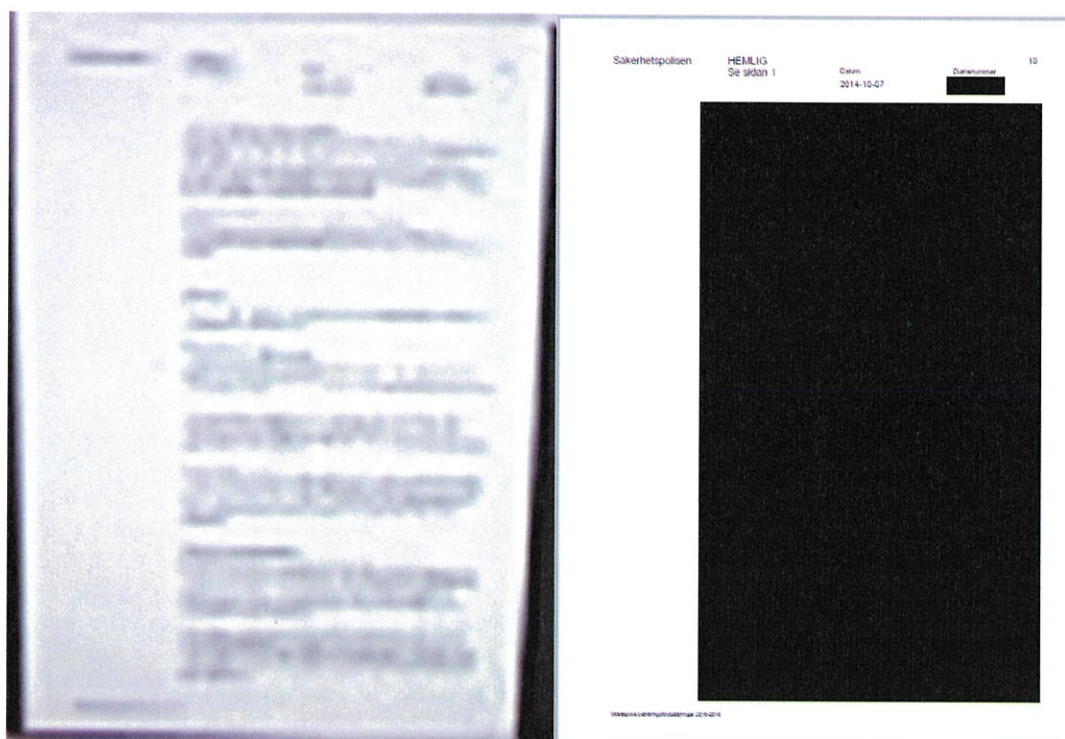


Säkerhetspolisen

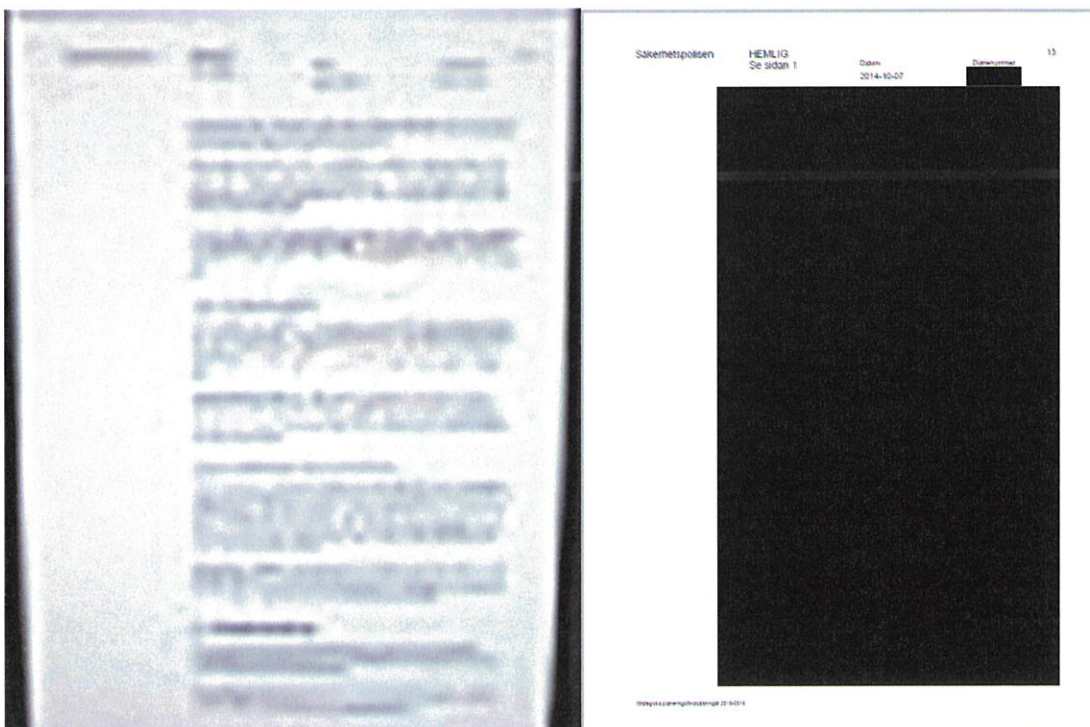
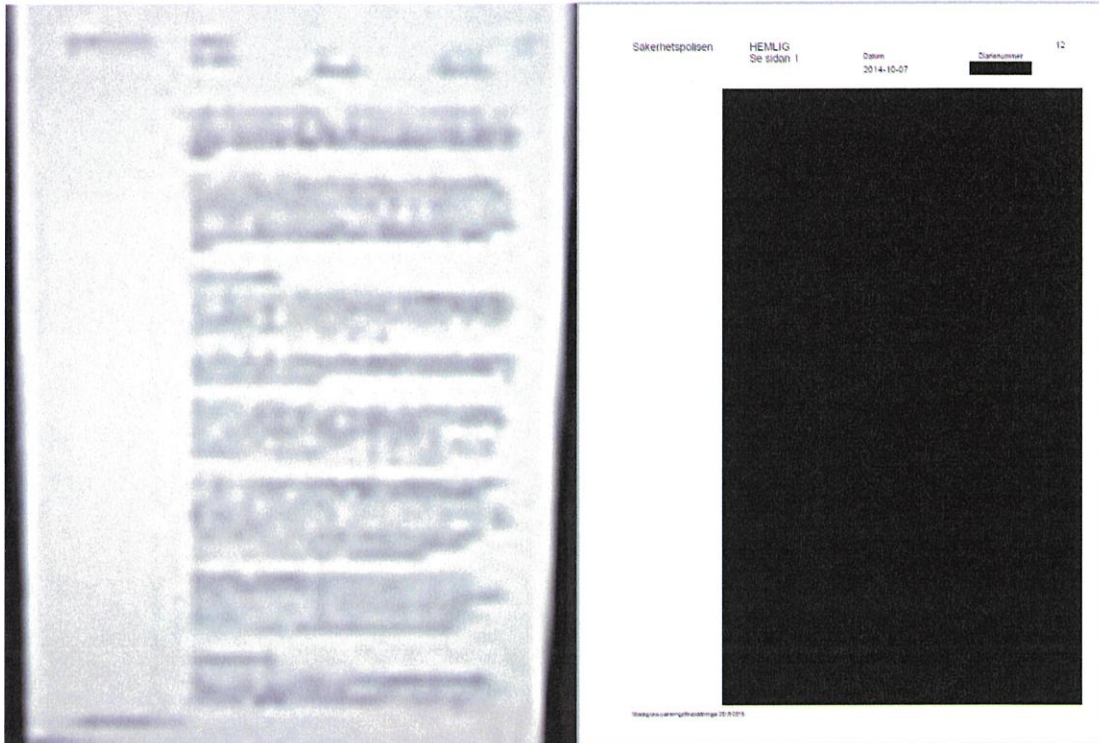
Datum: 2022-02-15

Diarienummer: 0105-K004-17

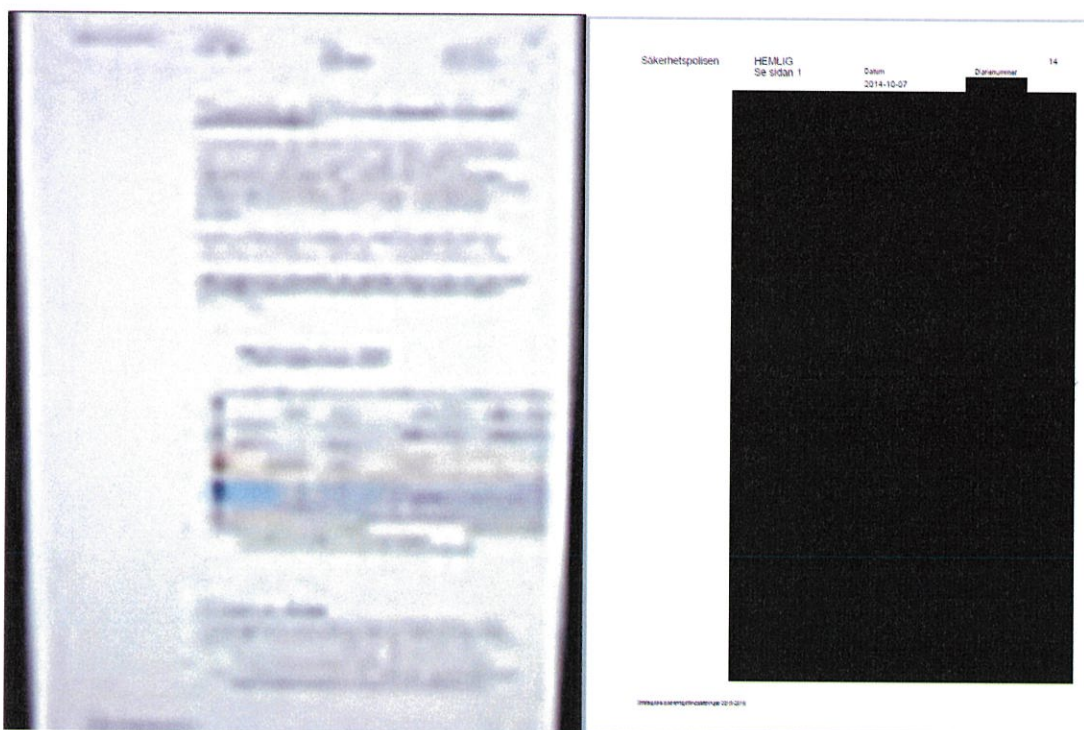
5(8)



Datum: 2022-02-15
Diarienummer: 0105-K004-17



Diarienummer: 0105-K004-17



	05127315	Typ: Bitmap Image Bildstorlek: 96 x 72	Storlek: 27,1 kB
	05127370	Typ: Bitmap Image Bildstorlek: 96 x 72	Storlek: 27,1 kB
	05127424	Typ: Bitmap Image Bildstorlek: 96 x 72	Storlek: 20,3 kB
	05127479	Typ: Bitmap Image Bildstorlek: 96 x 72	Storlek: 27,1 kB
	05127533	Typ: Bitmap Image Bildstorlek: 96 x 72	Storlek: 27,1 kB
	05127588	Typ: Bitmap Image Bildstorlek: 96 x 72	Storlek: 27,1 kB
	05127642	Typ: Bitmap Image Bildstorlek: 96 x 72	Storlek: 27,1 kB
	05127697	Typ: Bitmap Image Bildstorlek: 96 x 72	Storlek: 27,1 kB
	05127751	Typ: Bitmap Image Bildstorlek: 96 x 72	Storlek: 27,1 kB
	05127806	Typ: Bitmap Image Bildstorlek: 96 x 72	Storlek: 27,1 kB
	05127860	Typ: Bitmap Image Bildstorlek: 96 x 72	Storlek: 27,1 kB
	05127915	Typ: Bitmap Image Bildstorlek: 96 x 72	Storlek: 27,1 kB
	05127969	Typ: Bitmap Image Bildstorlek: 96 x 72	Storlek: 27,1 kB

Bildernas filnamn, i ordning (Tumnaqlarna har inga kända filnamn, det här är enbart löpnummer de fått vid åteskapandet).

Säkerhetspolisen

8(8)

Datum: 2022-02-15

Diarienummer: 0105-K004-17



Operativ handläggare

PM

Datum: 2022-08-29

Mottagare:

Diarienummer: -

Enhet:

Referens:

Namn: [REDACTED]

Titel:

Angående spår i Lenovo-datorn och Säkerhetspolisens utskriftsloggar

Inledning

Inom ramen för förundersökning 0105-K004-17 gällande misstanke om Grovt spioneri och Grov obehörig befattningsmed hemlig uppgift anträffades vid en husrannsakan 2021-09-20, i den misstänkte Peyman KIA ([REDACTED]) och dennes hustru Sarah [REDACTED] bostad på Hörnbovägen 2 i Uppsala, bland annat en bärbar dator av märke Lenovo (B063-21-24). Datorn togs i beslag och har därefter avbildats och undersökts av IT-forensiker. (Se IT-forensiskt undersökningsprotokoll i ärende 0105-K004-17).

Funnen information

Enligt undersökningsprotokollet från undersökningen av Lenovo-datorn (B063-21-24) framgår bland annat att det finns spår i datorn med nedan sökvägar och filnamn. (Se IT-forensiskt undersökningsprotokoll i ärende 0105-K004-17).

X:/	[REDACTED]	
X:/	[REDACTED]	
X:/	[REDACTED]	
X:/	[REDACTED]	

Enligt Säkerhetspolisens interna loggsystem över Peyman KIA:s aktiviteter i myndighetens nätverk, under perioden [REDACTED] [REDACTED] som registrerats som utskriftsaktiviteter. Se Excel-fil med de [REDACTED] utskriftsregistreringarna i sidomaterialet (0105-K004-17_logutdrag_ [REDACTED]).

Av dessa [REDACTED] utskriftsregistreringar har nedan fem loggrader valts ut då dessa utskrifter skulle kunna överensstämma med ovan information från Lenovo-datorn.

Datum: 2022-08-29

Diarienummer:

@timestamp	observer.product	event.code	host.hostname	message
Mar 2, 2011 @ 19:33:24.000	print	010	[REDACTED]	[REDACTED] 2011-03-02T19:32:54+01:00 030 2011-03-02T19:33:24+01:00 [REDACTED] print info [REDACTED] \PEY Dokumentet 56, Microsoft Word - [REDACTED] [REDACTED] gs av PEY skrevs ut p [REDACTED] HP LaserJet 1200 Series PCL via port [REDACTED] [REDACTED] Storlek i byte: [REDACTED] [REDACTED] Antal utskrivna [REDACTED] [REDACTED] info [REDACTED] [REDACTED] print info [REDACTED] \PEY Dokumentet 56, Microsoft Word - [REDACTED] [REDACTED] gs av PEY skrevs ut p [REDACTED] HP LaserJet 1200 Series PCL via port [REDACTED] [REDACTED] Storlek i byte: [REDACTED] [REDACTED] Antal utskrivna [REDACTED]
Mar 2, 2011 @ 19:33:36.000	print	010	[REDACTED]	[REDACTED] 2011-03-02T19:33:06+01:00 030 2011-03-02T19:33:36+01:00 [REDACTED] print info [REDACTED] \PEY Dokumentet 57, Microsoft Word - K [REDACTED] som [REDACTED] gs av PEY skrevs ut p [REDACTED] HP LaserJet 1200 Series PCL via port [REDACTED] [REDACTED] Storlek i byte: [REDACTED] Antal utskrivna [REDACTED] [REDACTED] info [REDACTED] [REDACTED] print info [REDACTED] [REDACTED] \PEY Dokumentet 57, Microsoft Word - [REDACTED] [REDACTED] som [REDACTED] gs av PEY skrevs ut p [REDACTED] HP LaserJet 1200 Series PCL via port [REDACTED] [REDACTED] Storlek i byte: [REDACTED] [REDACTED] Antal utskrivna [REDACTED]

Datum: 2022-08-29

Diarienummer:

@timestamp	observer.product	event.code	host.hostname	message
Mar 2, 2011 @ 19:33:59.000	print	010		2011-03-02T19:33:28+01:00 030 2011-03-02T19:33:59+01:00 print info \PEY Dokumentet 58, Microsoft Word - k som gs av PEY skrevs ut p HP LaserJet 1200 Series PCL via port Storlek i byte: Antal utskrivna info print info \PEY Dokumentet 58, Microsoft Word - som gs av PEY skrevs ut p HP LaserJet 1200 Series PCL via port Storlek i byte: Antal utskrivna
Mar 2, 2011 @ 19:34:17.000	print	010		2011-03-02T19:33:46+01:00 030 2011-03-02T19:34:17+01:00 print info 010 10 \PEY Dokumentet 59, Microsoft Word - gs av PEY skrevs ut p HP LaserJet 1200 Series PCL via port Storlek i byte: Antal utskrivna info print info 10 \PEY Dokumentet 59, Microsoft Word - som gs av PEY skrevs ut p HP LaserJet 1200 Series PCL via port Storlek i byte: Antal utskrivna

Datum: 2022-08-29

Diarienummer:

@timestamp	observer.product	event.code	host.hostname	message
Mar 2, 2011 @ 19:40:46.000	print	010		2011-03-02T19:40:16+01:00 030 2011-03-02T19:40:46+01:00 print info PEY Dokumentet 64, Microsoft Word - som gs av PEY skrevs ut p HP LaserJet 1200 Series PCL via port Storlek i byte: Antal utskrivna info print info PEY Dokumentet 64, Microsoft Word - som gs av PEY skrevs ut p HP LaserJet 1200 Series PCL via port Storlek i byte: Antal utskrivna



Datum: 2022-10-26

Diarienummer: -

Enhet:

Namn: [REDACTED]

Titel:

Mottagare:

Referens:

Angående Peyman KIA:s efterfrågan om information enligt mailkorrespondens i november 2009 och tillgång till Excelfilen '[REDACTED].xls' enligt Säkerhetspolisens datasystem (dataloggen/audit log).

Inledning

Inom ramen för förundersökning 0105-K004-17 gällande misstanke om Grovt spioneri och Grov obehörig befattning med hemlig uppgift har den misstänkte Peyman KIA:s ([REDACTED]) förehavanden i Säkerhetspolisens datasystem undersökts genom att granskning utförts av datasystemets loggning (audit log) för signaturen PEY respektive KIA¹.

Den dataloggning (audit log) som undersökts omfattar p [REDACTED] [REDACTED] loggningar (Excelrader). För den beskrivna perioden är bara signaturen PEY aktuell.

Mailkorrespondens 16-17 november 2009

[REDACTED]
[REDACTED]

I förundersökningsmaterialet finns information om mailkorrespondens där Peyman KIA efterfrågar information från Säkerhetspolisens ekonomienhet [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

¹ [REDACTED]
[REDACTED]
[REDACTED]

Datum: 2022-10-26

Diarienummer:

Funnen information

Vid sökning i Säkerhetspolisens loggningssystem (audit log) efter orden "██████████" framkommer att dessa ord finns med som en del i registrerade genvägar/pekare eller i filnamn i logghändelserna som kopplas till signaturen PEY.

Ett av sökorden, "██████████", träffar mot 10 logghändelser. I nedan tabell redovisas dessa 10 träffar i en förenklad form och i bilaga 1 redovisas träffarna i logghändelserna i sin helhet.

Datum	Tid	Sökväg	Åtkomster:
2010-04-28	09:52:22	██████████.x3	READ_CONTROL ReadData (or ListDirectory) WriteData (or AddFile) AppendData (or AddSubdirectory or CreatePipeInstance) %4419 WriteEA %4423 WriteAttributes
2010-04-28	09:52:25	██████████.LNK	READ_CONTROL ReadData (or ListDirectory) WriteData (or AddFile) AppendData (or AddSubdirectory or CreatePipeInstance) %4419 WriteEA %4423 WriteAttributes
2010-04-28	09:55:48	██████████	READ_CONTROL WriteData (or AddFile) AppendData (or AddSubdirectory or CreatePipeInstance) WriteEA %4423 WriteAttributes
2010-05-10	11:54:14	██████████	Accesses: DELETE %4423
2010-07-15	17:53:10	██████████.x3	READ_CONTROL ReadData (or ListDirectory) WriteData (or AddFile) AppendData (or AddSubdirectory or CreatePipeInstance) %4419 WriteEA %4423 WriteAttributes

Datum: 2022-10-26

Diarienummer:

Datum	Tid	Sökväg	Åtkomster:
2010-07-15	17:53:57	[REDACTED] LNK	READ_CONTROL ReadData (or ListDirectory) WriteData (or AddFile) AppendData (or AddSubdirectory or CreatePipeInstance) %4419 WriteEA %4423 WriteAttributes
2010-07-15	17:55:36	[REDACTED] .xls	READ_CONTROL WriteData (or AddFile) AppendData (or AddSubdirectory or CreatePipeInstance) WriteEA %4423 WriteAttributes
2010-07-15	17:55:48	[REDACTED] .xls	Accesses: DELETE %4423
2010-09-01	15:14:30	[REDACTED] LNK	Accesses: DELETE %4423
2010-09-01	15:14:30	[REDACTED] LNK	Accesses: DELETE %4423

Fem av träffarna är så kallade recent-genvägar [REDACTED] och fem av träffarna är fullständiga sökvägar till filen [REDACTED] (xls).

I kolumnen **Åtkomster:** redovisas behörigheten som signaturen PEY har gentemot filen.

Bedömning av tillgång till filen "[REDACTED].xls"

Utifrån aktuella logghändelser 2010-04-28, kl 09:52:22 – 09:52:25, bedöms det sannolikt att signaturen PEY öppnar filen "[REDACTED].xls". Bedömningen baseras på att både xls-filen och LNK-genvägen³ registreras i loggen inom en kort tidsrymd.

Utifrån logghändelser 2010-07-15, kl 17:53:10 – 17:53:57 bedöms det även här, på motsvarande grunder som ovan, att signaturen öppnar filen "[REDACTED].xls".

³ [REDACTED] LNK

Datum: 2022-10-26

Diarienummer:

Angående sökvägen till filen "[REDACTED].xls" enl audit-loggen för signaturen PEY

Sökvägen till filen "[REDACTED].xls" är:

[REDACTED].xls

Enligt sökvägen till filen är filen placerad i Säkerhetspolisens datasystem under Peyman KIA:s personliga mapp [REDACTED].

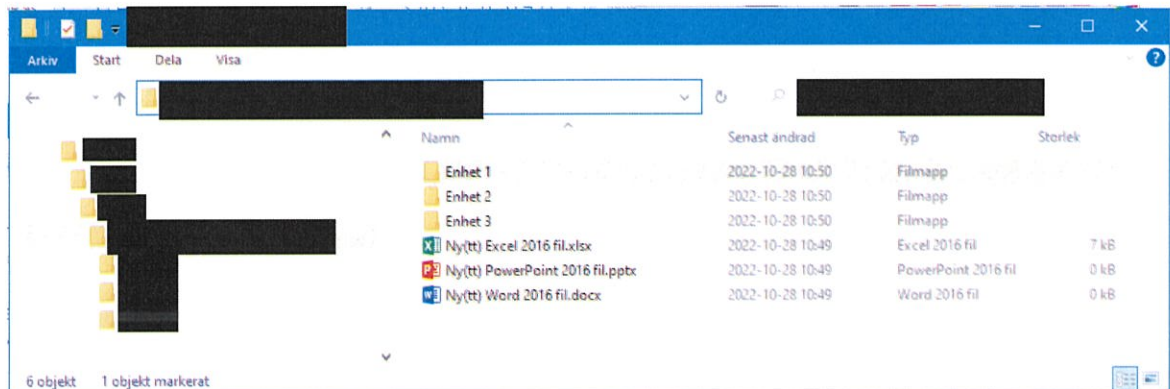
I sökvägen:

[REDACTED].xls

skulle delen "[REDACTED]" kunna indikera att filen legat i en gemensam mapp för myndighetsledningen på Säkerhetspolisen och att hela den mappen ([REDACTED]) med filer och eventuella undermappar kopierats till Peyman KIA:s egen personliga mapp "[REDACTED]".

Under mappen "[REDACTED]" finns ytterligare mappar och filer.

Nedan fiktiva bild försöker schematiskt åskådliggöra den beskrivna mappstrukturen.



Observera att ovan bild är fiktiv

Förutom filen "[REDACTED].xls" finns enligt loggningssystemet flera undermappar och filer under mappen "[REDACTED]". Se nedan bild.

Datum: 2022-10-26

Diarienummer:

Sökväg

Att mappen "[REDACTED]" följs av flera olika undermappar och filer bedöms stärka hypotesen att myndighetsledningens gemensamma mapp/mappar eller enskilda filer har kopierats ner till Peyman KIA:s egen personliga mapp [REDACTED].

I bilaga 2 finns en förteckning över logghändelserna till undermappar och filer, med datum och åtkomstbehörigheter, som påträffats i loggningssystem där sökvägen börjar med

[REDACTED]

Se bilaga 2.

Redogörelse för eftersök av filen "[REDACTED].xls" i Säkerhetspolisens datasystem.

2022-10-07 eftersöktes filen "[REDACTED].xls" i Säkerhetspolisens [REDACTED] samtliga filareor [REDACTED].

Sökningen genererade träff på filen "[REDACTED].xls" och återfanns på filarea:

[REDACTED]
[REDACTED].xls".

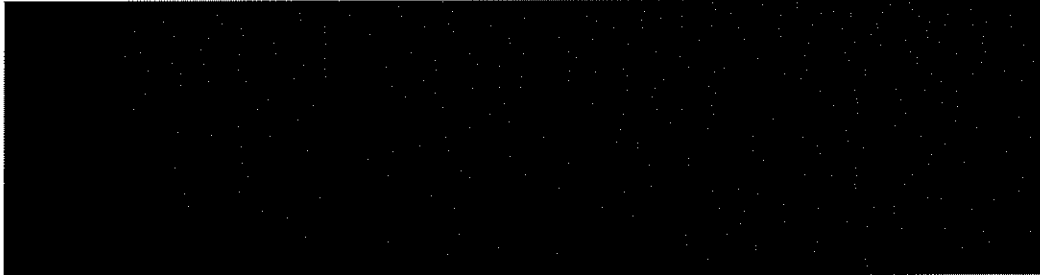
Skapandedatum enligt dokumentets metadata är 2009-05-28. Den funna filen, med namnet "[REDACTED].xls", är den enda nu existerande filen med namnet "[REDACTED].xls" i Säkerhetspolisens [REDACTED].

Datum: 2022-10-26

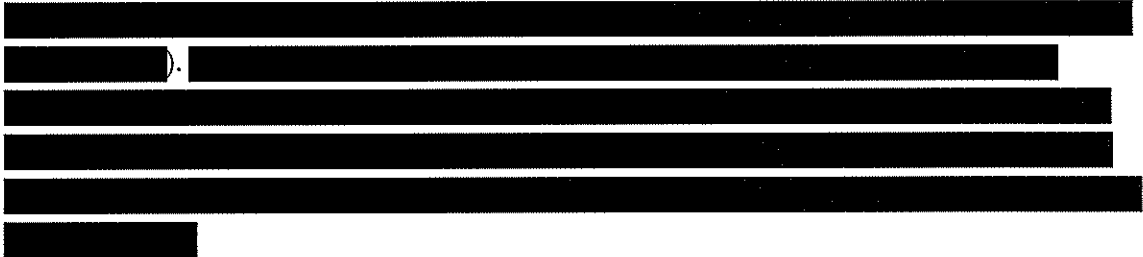
Diarienummer:

Beskrivning av filen "[REDACTED].xls" som påträffades 2022-10-07 i i Säkerhetspolisens datasystem.

Filen "[REDACTED].xls" är en Excelfil med sex blad. Bladens namn är:



På respektive blad finns information i kolumner med kolumnnamnen



Förteckningen i filen "[REDACTED].xls" listar [REDACTED] vid Säkerhetspolisens [REDACTED]

I bilaga 3 redovisas ett typexempel över hur informationen är strukturerad i samtliga [REDACTED]

Redogörelse för vilka som hanterar information som återfinns i filen

"[REDACTED].xls"

I en separat PM i förundersökningen redogörs för vilka som normalt hanterar information som återfinns i filen "[REDACTED].xls". Se PM "Beskrivning [REDACTED]

[REDACTED] Säkerhetspolisen, ärende 0105-K004-17".

Diarienummer:

Bilaga 1

ordet Accesses: har gulmarkerats för att lättare återfinnas i nedan tabell.

@timestamp	observer.product	event.code	host.hostname	message
Apr 28, 2010 @ 09:52:22.000	security	0560	[REDACTED]	[REDACTED]
Apr 28, 2010 @ 09:52:25.000	security	0560	[REDACTED]	[REDACTED]

Datum: 2022-10-26

Diarienummer:

@timestamp	observer.product	event.code	host.hostname	message
Apr 28, 2010 @ 09:55:48.000	security	0560	[REDACTED]	[REDACTED]
May 10, 2010 @ 11:54:14.000	security	0560	[REDACTED]	[REDACTED]

Datum: 2022-10-26

Diarienummer:

@timestamp	observer.product	event.code	host.hostname	message
Jul 15, 2010 @ 17:53:10.000	security	0560	[REDACTED]	[REDACTED]
Jul 15, 2010 @ 17:53:57.000	security	0560	[REDACTED]	[REDACTED]

@timestamp	observer.product	event.code	host.hostname	message
Jul 15, 2010 @ 17:55:36.000	security	0560	[REDACTED]	[REDACTED]
Jul 15, 2010 @ 17:55:48.000	security	0560	[REDACTED]	[REDACTED]
Sep 1, 2010 @ 15:14:30.000	security	0560	[REDACTED]	[REDACTED]

Datum: 2022-10-26

Diarienummer:

@timestamp	observer.product	event.code	host.hostname	message
Sep 1, 2010 @ 15:14:30.000	security	0560		

Datum: 2022-10-26

Diarienummer:

Bilaga 2

I nedan tabell, baserad på logghändelserna (audit log), redovisas alla recent-genvägar och sökvägar till filer som innehåller texten "[REDACTED]" i sökvägen.

Datum och antal av 'Accesses:' Client User Name: PEY	READ_CONTROL ReadData (or ListDirectory) WriteData (or AddFile) AppendData (or AddSubdirectory or CreatePipeInstance) %4419 WriteEA %4423 WriteAttributes	READ_CONTROL WriteData (or AddFile) AppendData (or AddSubdirectory or CreatePipeInstance) WriteEA %4423 WriteAttributes	Accesses: DELETE %4423	DELETE READ_CONTROL WriteData (or AddFile) AppendData (or AddSubdirectory or CreatePipeInstance) WriteEA %4423 WriteAttributes	Totalsumma
2010-04-28					
[REDACTED] LNK	2		1		3
[REDACTED] xls	1	1			2
[REDACTED] xls	1	1			2
[REDACTED] xls	1	1			2
[REDACTED] xls	1	1			2
[REDACTED] xls	1	1			2
2010-05-05					
[REDACTED] LNK			1		1
2010-07-15					
[REDACTED] LNK	8		7		15
[REDACTED] xls	2	2	1		5
[REDACTED] xls	2	2	1		5
[REDACTED] ppt	1		1		2

Datum: 2022-10-26

Diarienummer:

Datum och antal av 'Accesses:' Client User Name: PEY	READ_CONTROL ReadData (or ListDirectory) WriteData (or AddFile) AppendData (or AddSubdirectory or CreatePipeInstance) %4419 WriteEA %4423 WriteAttributes	READ_CONTROL WriteData (or AddFile) AppendData (or AddSubdirectory or CreatePipeInstance) WriteEA %4423 WriteAttributes	Accesses: DELETE %4423	DELETE READ_CONTROL WriteData (or AddFile) AppendData (or AddSubdirectory or CreatePipeInstance) WriteEA %4423 WriteAttributes	Totalsumma
[REDACTED] [REDACTED].doc	1	1	1		3
[REDACTED] [REDACTED].xls	2	2	1		5
[REDACTED] [REDACTED].doc	1		1		2
[REDACTED] [REDACTED].xls			1		1
[REDACTED] [REDACTED].xls			1		1
[REDACTED] [REDACTED].xls			1		1
[REDACTED] [REDACTED].xls	1	1	1		3
[REDACTED] [REDACTED].xls			1		1
[REDACTED] [REDACTED].xls	1	1	1		3
[REDACTED] [REDACTED].xls	1	1	1		3
[REDACTED] [REDACTED].doc			1		1
[REDACTED] [REDACTED].xls			1		1
[REDACTED] [REDACTED].ppt			1		1
[REDACTED] [REDACTED].xls	1	1	1		3

Datum: 2022-10-26

Diarienummer:

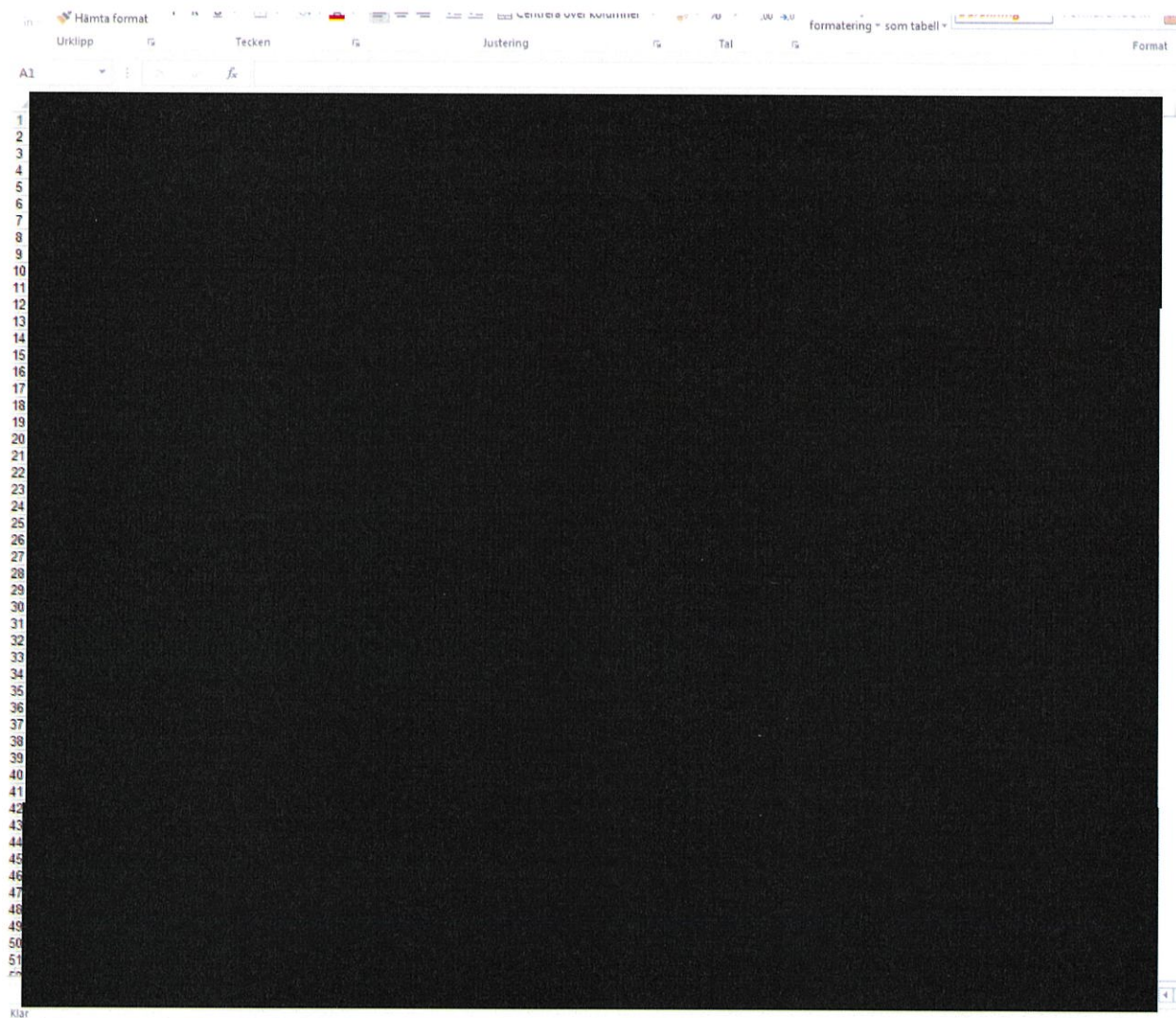
Datum och antal av 'Accesses:' Client User Name: PEY	READ_CONTROL ReadData (or ListDirectory) WriteData (or AddFile) AppendData (or AddSubdirectory or CreatePipeInstance) %4419 WriteEA %4423 WriteAttributes	READ_CONTROL WriteData (or AddFile) AppendData (or AddSubdirectory or CreatePipeInstance) WriteEA %4423 WriteAttributes	Accesses: DELETE %4423	DELETE READ_CONTROL WriteData (or AddFile) AppendData (or AddSubdirectory or CreatePipeInstance) WriteEA %4423 WriteAttributes	Totalsumma
[REDACTED].pdf			1		1
[REDACTED].xls	1	1	1		3
[REDACTED].xls	1	1	1		3
[REDACTED].xls	1	1	1		3
[REDACTED].xls	1	1	1		3
[REDACTED].ppt			1	1	2
[REDACTED].ppt				1	1
2010-07-22					
[REDACTED].LNK			1		1
2011-03-02					
[REDACTED].ppt			1		1
Totalsumma	32	20	34	2	88

Datum: 2022-10-26

Diarienummer:

Bilaga 3

Nedan bild redovisar strukturen på informationen för respektive blad i filen [REDACTED]. Den riktiga filen innehåller [REDACTED]



Datum: 2022-11-03
Diarienummer: [REDACTED]
Enhet:
Namn: Martin Wagner
Titel: Säkerhetschef

Mottagare:

Referens:

Beskrivning av [REDACTED] Säkerhetspolisen,
ärende 0105-K004-17

Sammanfattning

I Säkerhetspolisens ärende 0105-K004-17

Beskrivning av handlingen

[REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]

[REDACTED]

Datum: 2022-11-03

Diarienummer:

[REDACTED]

Martin Wagner
Säkerhetschef

Säkerhetspolisen

Datum: [2022-11-03]

Diarienummer: [0105-K004-17]

Titel: [Protokollbilaga D.2 – bilaga till IT-forensiskt
undersökningsprotokoll]



Sakerhetspolisen • Box 12312 • 102 28 Stockholm
Tfn: 010-568 70 00 • Fax: 010-568 70 10
E-post: sakerhetspolisen@sakerhetspolisen.se
www.sakerhetspolisen.se