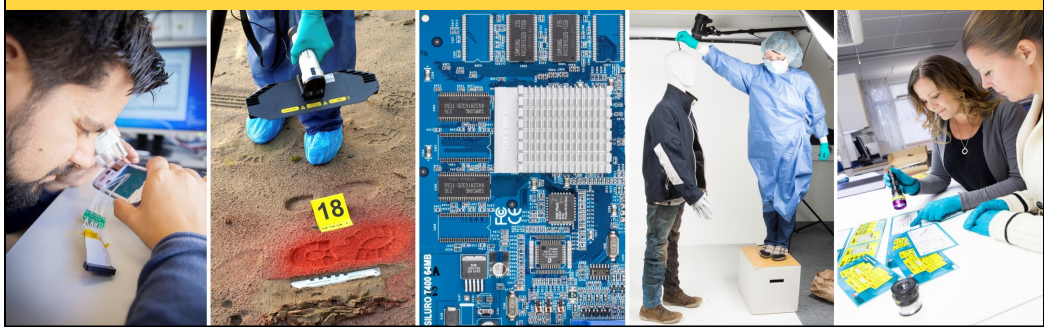
Polisen

Mobil, elektronik och dator

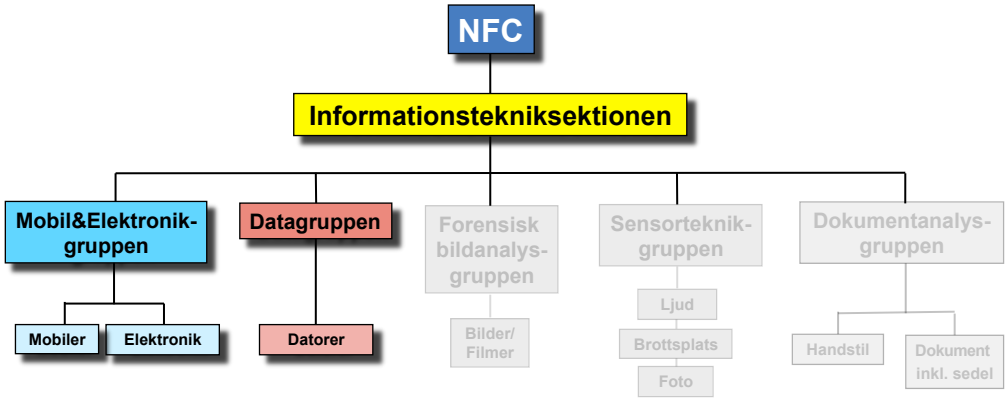
2018-05-22, Tommy Färnqvist, NFC



IT-relaterad brottslighet (BRÅ)

- IT är ***målet*** och en förutsättning för brottets genomförande, till exempel dataintrång.
- IT är ***medlet*** och har understött brottet, till exempel genom att ett socialt forum används för att hota någon.
- IT kan, utan att vara mål eller medel, ha ***beröring*** med brottet. Detta genom att digitala spår har lämnats som kan användas som bevisning vid ett brott som har begåtts utanför IT-miljö.

(Från BRÅs rapport ”It-inslag i brottsligheten och rättsväsendets förmåga att hantera dem”, 2016:17)

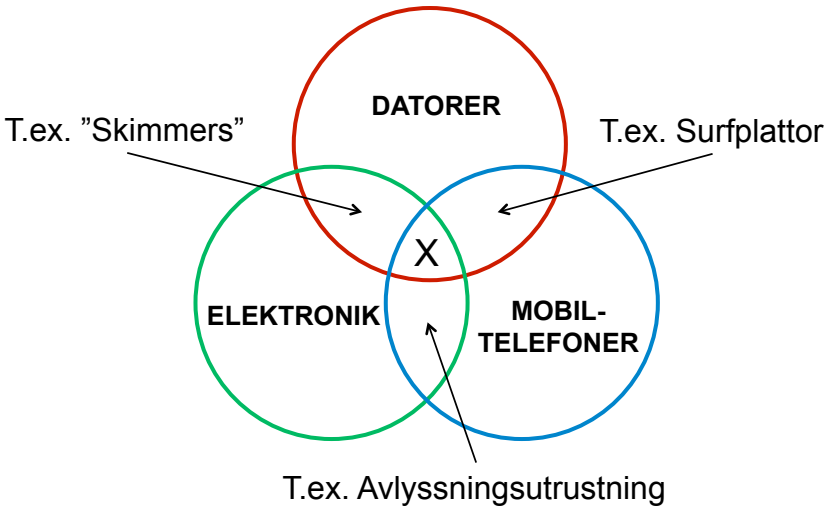


Polisen

Data-, elektronik- och mobilundersökningar

- Våra områden
- Våra undersökningar
- Utmaningar vi stöter på
- Exempel på ärenden
- Framtidsområden

Polisen



Polisen

X = T.ex. bilelektronik

Vad vi gör

Undersökningar
Ärenden

Metodutveckling
T.ex. inom dekryptering

Expertstöd
Kompetensbank åt rättsväsendet

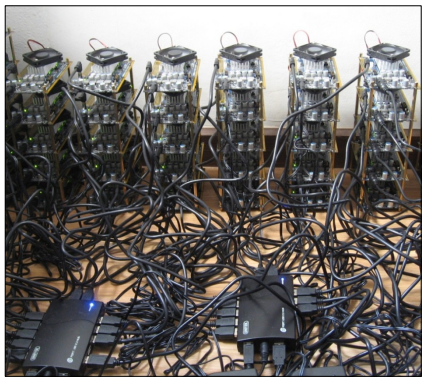
Polisen

Kvalitet

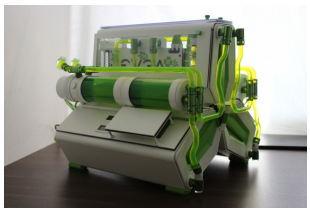
- Ackrediterade på IT-undersökningar
- Validering av metoder (vilka inkluderar verktyg)
- Kontroll av resultat med flera verktyg
- Medgranskning av resultat

Datagruppen (datorer och databärare)

- Dataextraktion/analys
- Reparation
- Funktionsanalys
- Mjukvaruanalys
- Platsundersökningar



Utmaningar



Unika ärenden

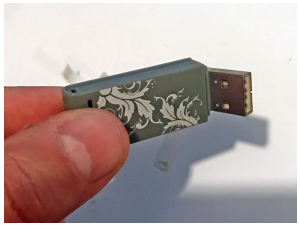
Stora datamängder

Lösenord/Kryptering

Polisen

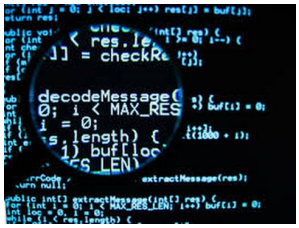
Fokusområden för framtiden

Dataextraktion



Dekryptering

Mjukvaruanalys



Polisen

Exempel på ärende – kraschad drönare

Bild borttagen

Exempel på ärende – kraschad drönare

Bild borttagen

Exempel på ärende – kraschad drönare

Bild borttagen

Exempel på ärende – kraschad drönare

Bild borttagen

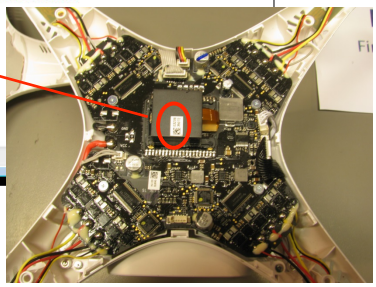
Exempel på ärende – kraschad drönare

Bild borttagen

Exempel på ärende – kraschad drönare

Från .CONFIG.TXT-fil på ”Svarta Lådan”

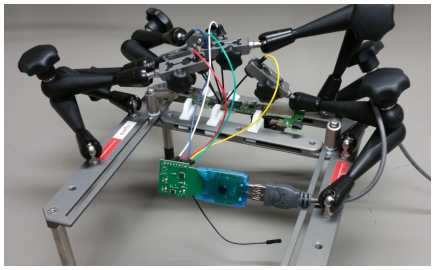
```
12488 : [     20.000000] => g_config.bat_limit.limit_power_rate_temp.weight_0
12500 : [ 35000.000000] => g_config.bat_limit.limit_bat_current_after_overflow_0
12512 : [      0.500000] => g_config.bat_limit.limit_up_rate_0
12524 : [      0.100000] => g_config.bat_limit.limit_down_rate_0
12524 : Mc  ID  :03Z0935072
12524 : Mc  Ver :v2.4.14.5
12524 : Bat Ver :v255.255.255.255
12524 : Svn Ver :9566
12524 : Time    :2016-03-29 20:59
171981 : [ 1]App Cmd 12
270345 : [ 1]App Cmd 12
665613 : [ 1]App Cmd 12
```



MC ID visar drönarens serienummer. Återfinns även på drönarens MCU på moderkortet, samt i DJI Flight Record-loggarna på mobilenheten.

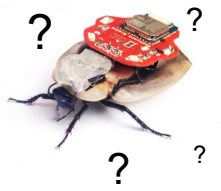
Mobil- och Elektronikgruppen (Elektronik)

- Dataextraktion/analys
- Funktionsanalys



Polisen

Utmaningar



Unika ärenden

Lösenord/Kryptering

Polisen

Exempel på ärende – eldosan

Bild borttagen

Bild borttagen

IOT-Forensik

- Vad är IOT?
  - **Internet of Things (IoT)** är definierat som en global infrastruktur för informationssamhället, som möjliggör avancerade tjänster genom att sammankoppla (fysiskt och virtuellt) saker som bygger på befintlig och kommande informations- och kommunikationsteknik.
- Exempel
  - Smarta hem-tillbehör, t.ex. smarta lås, sensorer för temperatur, omgivande ljus, vatten etc.
  - Smarta klockor, smarta glasögon, pacemaker samt träningsredskap kan t.ex. innehålla M2M-kommunikation samt RFID

IOT-Forensik

- Vad är IOT-forensik?
  - Ett ganska så nytt område, som inte i någon större grad utforskats m.a.p. vilken information som kan hämtas ut.
  - IOT är en undergrupp till digital forensik och kräver ett mångfacetterat tillvägagångssätt där bevis kan samlas in från en rad olika källor, t.ex. sensorer, kommunikationsenheter, molnlagring samt ISP-loggar.
- Exempel
  - Är det möjligt att se när den smarta klockan gjorde så att användaren loggades in på datorn?
  - Vad spelar Alexa in och hur fås denna information ut?
  - Är det möjligt att se vilken tid som ytterdörren låstes upp och av vem?
  - Har systemet blivit hackat?

IOT-forensik

- Riktigt fall: Amazon Echo (Nov 2015)
  - Polisen i Arkansas beslagtog Bates' Echo från hans hem och polisen begärde av Amazon att överlämna information angående enhetens kommunikation med Alexa Cloud.
  - https://edition.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/index.html

Bil-forensik

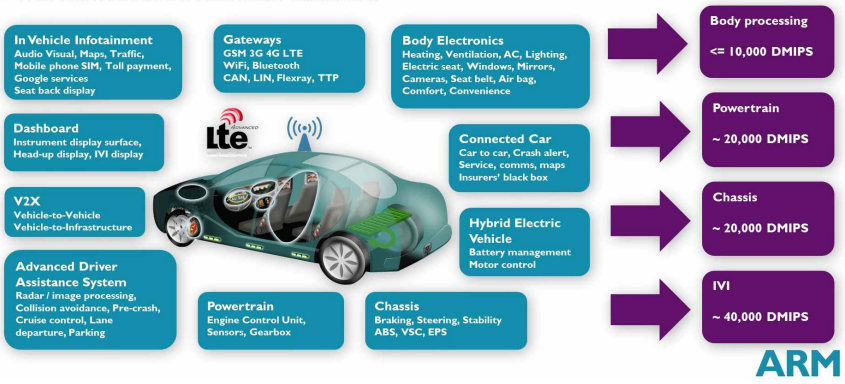
- När bromsade bilen?
- När öppnades bildörren?
- Bränslenivåer?

- Listan kan göras lång….

Bil-forensik

Automotive ECUs Controllers by 2020

- Between 25 and 100 individual ECUs
- With distributed sensors and motor controllers.



Bil-forensik i framtiden?

- Självkörande bilar
- Uppkopplade bilar
- Ännu högre mängd av sensorer.

- Vilken typ av bevis kan vi hitta?

Mobil- och Elektronikgruppen (Mobilenheter)

- Preparering
- Extrahering och tolkning
- Analys

Polisen

Utvecklingen!

”Digitala beteendearkiv”

Polisen

Typer av mobila enheter

Ringtelefoner	Funktionstelefoner	Smartmobil	Wearables
Enkel funktion	Förutbestämda applikationer	Användarstyrda applikationer	Smart watch m.m.
	- Röst - SMS - Kamera - Internet - E-post - Kalender - Alarm	- Förinstallerade appar - Store	

Polisen

Undersökning av mobilenheter vs datorer

Mobil och elektronik

Inbäddade system

Data

Analys data

Polisen

Preparering – exempel

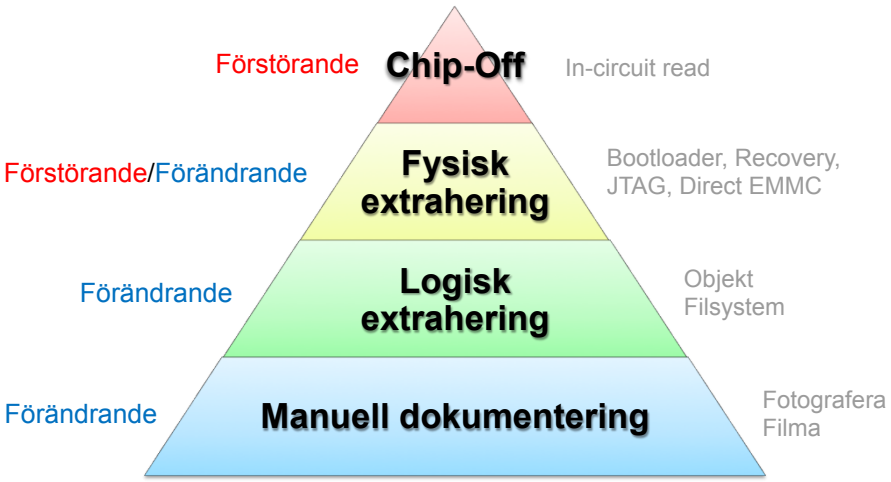
Brandskadadade, vattenskadade,
förstörda med vilje, besudlade (blod, vätska)

”Går det att få ut någon information ur telefonen?”

Bild borttagen

Polisen

Extraheringar



Polisen

Analys – utmaningar

Android → ACD → OEM → Modell → App

233 versioner mellan juni 2014 och oktober 2017

47 versioner av Android 5 ”Lollipop”

70 versioner av Android 6 ”Marshmallow”

103 versioner av Android 7 ”Nougat”

13 versioner av Android 8 ”Oreo”

Android Compability Definition

MUST…
MUST NOT…
REQUIRED…
SHALL…
SHALL NOT…
SHOULD…
SHOULD NOT…
RECOMMENDED…
MAY…
OPTIONAL…

HUAWEI, ONEPLUS, BlackBerry, NOKIA, MOTOROLA, SAMSUNG, htc, SONY, LG

Samsung

Galaxy Note – Pumped up

Galaxy S – ”High end”

Galaxy A – ”Mid range”

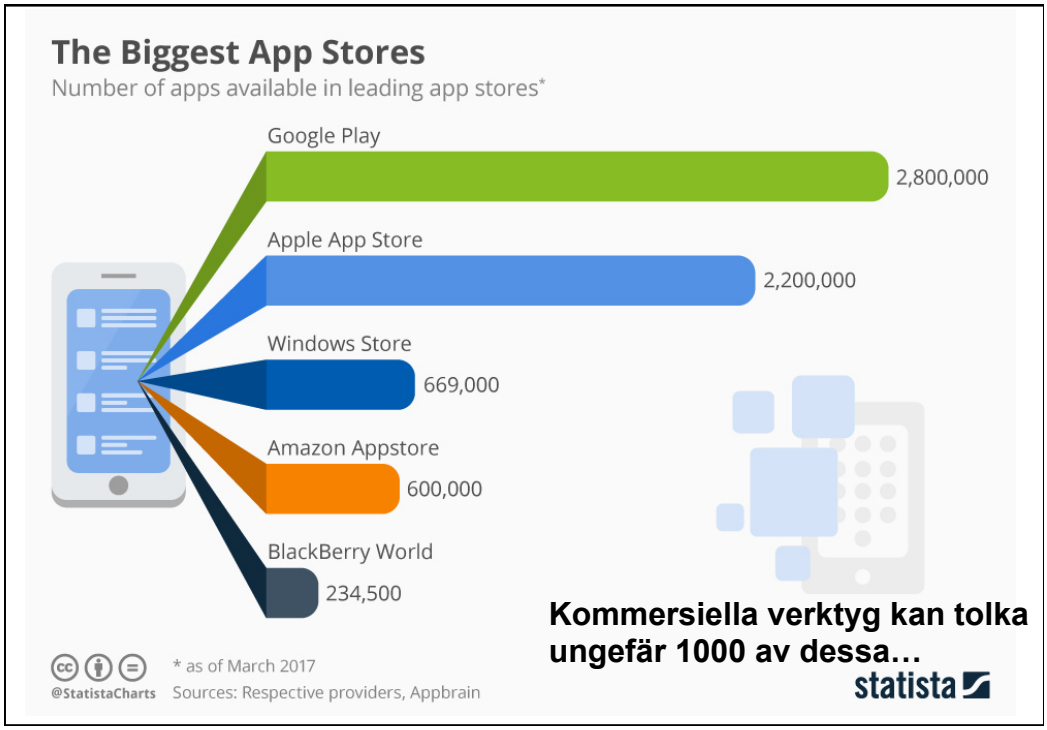
Galaxy J – ”Low end”

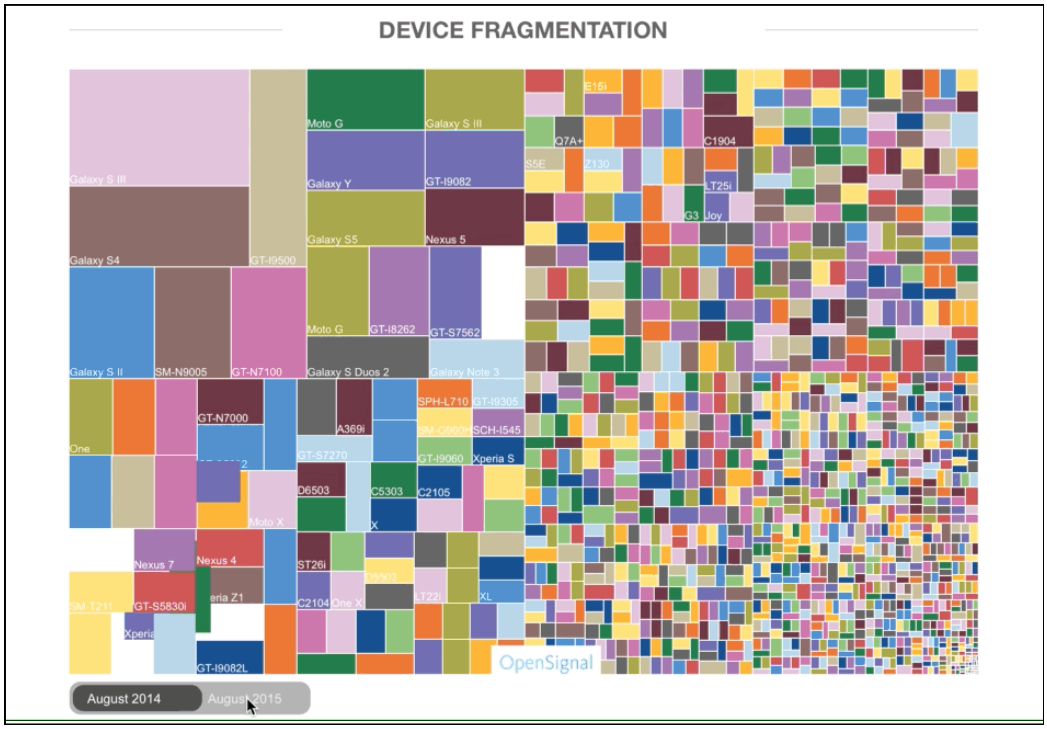
128 versioner mellan juni 2014 och oktober 2017

Polisen

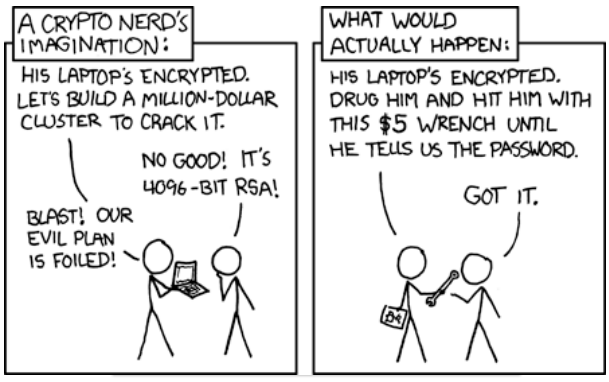
33

2018-05-22





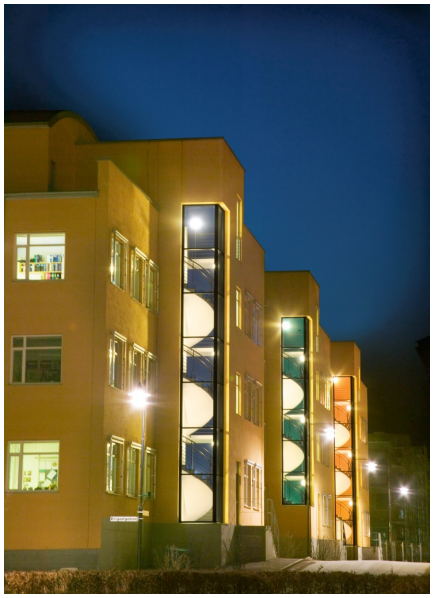
Säkerhet – utmaning och utvecklingsområde



Er uppgift – enkel applikationsanalys

- Vilken/vilka metoder anropas metoden
  `com.mywickr.wickr.WickrMessage.getMessagePayload()`
  av i version 4.33.4 av appen Wickr Me Private Messenger?
  - Redogör för ditt val av verktyg samt metodik.

Polisen



Frågor?

Polisen