

1 Doel

Deze procedure beschrijft de werkwijze van een technische intake hardware in het kader van onderzoekswerk, productcodes: DTE001, DTE006, DTE210. Het fotograferen, documenteren en openen van mobiele telefoons en andere consumentenelektronica. Let op: DTE004 onderzoeken worden niet volgens dit werkvoorschrift ingeboekt. Onder DTE004 valt o.a.:

- reparatie, hier is het inboeken sterk afhankelijk van de toestand van de telefoon en wordt beschreven in werkvoorschrift DTE004.
- Device live forensics, hiervoor moet de telefoon aan blijven staan

2 Procesbeschrijving

	Legenda		
	1 ⚠ 💡	Proces stap visueel Let op Tip/ idee	🖨 ✉
			Printen Brief/ mail maken

	Processtappen	Visuele ondersteuning	Best practices/Tips
1	De eerste stap is administratief inboeken, zie <i>FDT – DTE210 Intake hardware Support</i> . Als er nog geen zakenmap is aangemaakt kan dit worden gedaan via 5.1.2i 5.1.2i		Scan zaaknummer en SVO nummers in met de barcode reader.
2	⚠ 💡 Prepareer een ESD zak, bijv. NEFAB BBAS7210, 15x25 cm, of equivalent, met zaaknummer, SIN-deelsticker en ESD - waarschuwingssticker. Hierin wordt de PCB straks verpakt.		De medewerker is bekend met en werkt gedurende deze hele procedure volgens het NFI ESD beleid, ESD - polsband en -schoenen.
2A	⚠ Controleer of het afvoerkistje voor gevaarlijke batterijen aanwezig is. Zo ja, ga naar 2B		Als de telefoon in punt 3B een batterij bevat, ga dan alleen verder als het kistje er is.
2B	Controleer of de systeemtijd op de camera en op de PC goed staan. Doe dit met: - Atoomklokontvanger - www.time.gov Mocht de PC- tijd niet goed staan, moet er een melding via het stafloket gemaakt worden. Als de tijd op de camera aangepast moet worden kun je dit vinden in de handleiding	Let op, www.time.gov geeft de UTC tijd (rechts boven in het scherm). Nederland loopt één of twee uur voor op die tijd. Noteer in JIRA of op het WNF dat de tijd is gecontroleerd.	

	5.1.2i														
2C 	Controleer of er specifieke voorschriften zijn voor dit model telefoon.	Google Pixel	Zie Google Pixel3a/4(a) phones with FBE: Case Procedures												
3  	Pak het SVO uit en fotografeer iedere laag van de verpakking van het SVO. Bij een enveloppe voor en achterzijde, bij een doos alle zijden waar iets op vermeld staat. Alle verpakkingen dienen bewaard en retour gezonden te worden naar de aanvrager! LET OP: Bij het aantreffen van een RISICO - sticker, onmiddellijk stoppen en onderzoeken wat dit risico inhoudt. Redenen van RISICO - sticker kunnen zijn: Bloed (opgedroogd), andere lichaamsvloeistoffen, chemische verontreiniging, etc. Overleg met de zaakverantwoordelijke over hoe verder te gaan. Evt DTE004 om SVO te reinigen.		Fotografeer zoveel mogelijk met een fotoliniaal en het zaaknummer en/of SIN in beeld. Controleer of de foto's scherp zijn. Ook lege verpakkingen, zakjes of dergelijken.  Draag beschermende handschoenen waar nodig.  Vermijdt het indrukken van toetsen. Als het toestel inschakelt kan informatie worden gewist.  Sluit geen kabels aan, dit kan anti-forensische wis-acties triggeren.												
3A 	Voor toestellen met ingebouwde batterij: Controleer of het toestel echt uit is. Let op, voor DTE004 / Live forensics geldt dit niet	<table><tr><th>Merk/serie</th><th>Actie</th></tr><tr><td>BlackBerry, OS<10</td><td>Druk op  toets</td></tr><tr><td>BlackBerry, OS=10 Met toetsenbord</td><td>Druk op willekeurige toets op toetsenbord</td></tr><tr><td>BlackBerry, OS=10 Met touchscreen only</td><td>Swipe van beneden naar boven over touch screen</td></tr><tr><td>Apple iPhone</td><td>Schakel 'stil' toets, toestel trilt als het aan staat</td></tr><tr><td>Android generiek</td><td>Druk kort op de volume</td></tr></table>	Merk/serie	Actie	BlackBerry, OS<10	Druk op  toets	BlackBerry, OS=10 Met toetsenbord	Druk op willekeurige toets op toetsenbord	BlackBerry, OS=10 Met touchscreen only	Swipe van beneden naar boven over touch screen	Apple iPhone	Schakel 'stil' toets, toestel trilt als het aan staat	Android generiek	Druk kort op de volume	
Merk/serie	Actie														
BlackBerry, OS<10	Druk op  toets														
BlackBerry, OS=10 Met toetsenbord	Druk op willekeurige toets op toetsenbord														
BlackBerry, OS=10 Met touchscreen only	Swipe van beneden naar boven over touch screen														
Apple iPhone	Schakel 'stil' toets, toestel trilt als het aan staat														
Android generiek	Druk kort op de volume														

			knop
		Overige merken/modellen, overleg met zaakverantwoordelijke	
3B 	Controleer of de batterij in de telefoon verdacht is. Ja: doe de telefoon in het afvoerkistje en ga onmiddellijk naar ruimte 5.1.2i Werk verder in de zuurkast aldaar. Nee: ga na of <u>de batterij problemen kan geven bij verwijderen</u>, bijvoorbeeld omdat je met gereedschap moet wrikken om hem los te krijgen, of <u>als je niet weet hoe de batterij los moet</u> Ja: ga naar ruimte 5.1.2i en werk verder in de zuurkast aldaar met punt 4A Nee: ga naar 4A.		Verdacht is: Telefoon vertoont schade aan de buitenkant, is doorboord, gebogen/gebroken, stinkt, etc. OF Batterij - staat bol - stinkt
3C	Als je in ruimte 5.1.2i werkt ivm verdachte batterij, controleer de werking van de pyrometer, je huid zou rond de 35 graden moeten zijn.		
3D	De batterij staat bol of stinkt.	In telefoons met een batterij die bol staat of stinkt: Plaats de batterij in de munitiekist en breng deze naar dock 3, daar kan de batterij worden afgevoerd. https://inception.nfi.minjus.nl/index.jsp?bookmark=ID%3D1000145	
3E	De batterij is te heet, sist, rookt of brandt	Als de batterij tijdens het uitpakken/uitprepareren onverhoopt in brand vliegt of daar tekenen van vertoont (heet worden, roken, sissen, bol gaan staan of stinken) dan laat je hem vallen, liefst in de stalen bak, trek je onmiddellijk de klep van de zuurkast dicht, verlaat (met eventuele anderen) de ruimte en bel je 5.1.2e of 5.1.2e (via een vaste telefoon). Ga er niet mee rondlopen! De brandtemperatuur van zo'n batterij is heel hoog en er komen giftige gassen waaronder waterstoffluoride bij vrij. In extreme gevallen kan de batterij zelfs ontploffen.	
4A	Als het SIN - moederfel (met de RFID antenne los bij de verpakking zit, plak deze dan op de laatste verpakking van het SVO, Dit om te voorkomen dat de losse stickervellen	Plak de RFID sticker niet op een ESD zakje, deze werkt daardoor niet meer!	

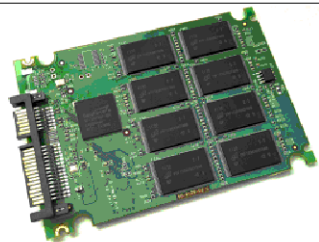
FDT - Technische intake hardware

	gescheiden raken van het SVO. Maak een extra foto van SIN moedervel op verpakking.	
4B	Controleer of er items mee verpakt zijn (bijv. sim kaart, sd kaart, etc) die wel een SIN hebben, maar die niet zijn ingeboekt in PROMIS.	Frontdesk pakt uit tot aan de eerste SIN - sticker. Als daarbinnen nog een extra item met SIN zit, dan zien ze die niet. Vooral nu politie geen RFID - stickers meer gebruikt. Als er zulke niet ingeboekte items zijn, laat deze dan alsnog inboeken door frontdesk.
5	Fotografeer voor- en achterzijde van het SVO. Maak detailfoto van eventuele kenmerkende gegevens op de buitenzijde (merk/type serienummer, IMEI). Fotografeer deze kenmerkende gegevens op de verpakking met het "In Beslagname Nummer", SIN -sticker en NFI -zaaknummer sticker duidelijk in beeld. Hiermee wordt in één foto de relatie gelegd tussen de originele nummering van de politie tijdens in beslagname en een IMEI, serienummer e.d. . Wjsg	
5A	Plak eventueel aanwezig camera's op voor- en achterzijde af met een stickertje.	Om te voorkomen dat per ongeluk foto's gemaakt worden van omgeving of onderzoekers. Zie ook VH-2020-177.
6	Demonteer het SVO wanneer dat kan. Neem bijvoorbeeld batterijklep af en verwijder batterij. 	Overleg met de onderzoekverantwoordelijke wanneer je niet zeker bent of de batterij verwijderd mag worden.
7	Bij inboeken in JIRA moeten alle kenmerken van de mobiele telefoon worden opgegeven. Zie deze pagina voor details oer wat in te voeren in JIRA. Inclusief een subpage voor labels: https://confluence.dev.holmes.nl/display/DT/Jira+invoeren+bij+start+onderzoek 	
7a	Geef in JIRA ook aan mbv labels REPAIR, CRYPTO, EXPLOIT of CHIPS naar welke subteam de zaak het eerst gaat.	
8	Maak een overzichtsfoto met gedemonteerde batterij en klep. Maak detailfoto van eventuele kenmerkende gegevens op de buitenzijde (merk/type serienummer IMEI). Fotografeer kenmerkende gegevens met de SIN sticker duidelijk in beeld.	

9 	SIMKAART: Als er simkaart(en) aanwezig is(zijn), verwijder deze, noteer de provider(s) en kaartnummer(s) van de simkaart(en) in JIRA (SVO) en fotografeer deze, met SIN - sticker zichtbaar. Als er geen simkaart aanwezig is en als de simkaart houder niet duidelijk als leeg te zien is in punt 9, fotografeer deze dan nogmaals in detail.		
9a	Berg de simkaart(en) op in een klein ESD zakje ($\approx 4 \times 6$ of 5×8 of 8×12 cm), en plak er een SIN - sticker op of schrijf het SIN erop. Dit zakje moet in de originele verpakking waar de RFID sticker op zit.		
9b	Maak een foto van het zakje met de SIN (sticker) en simkaart(en) zichtbaar er in		Als het niet mogelijk is met de Canon Powershot G5X MarkII om van het kenmerken een foto te maken. Neem dan een andere camera met scheerlicht. Vergeet niet deze foto ook in de zakenmap te plaatsen.
10  	Als er een geheugenkaart aanwezig is, verwijder deze, noteer merk, type, serienummer, capaciteit en overig opschrift in JIRA (SVO) en fotografeer deze, met SIN - sticker zichtbaar. Als er geen geheugenkaart aanwezig is en als de geheugenkaart houder niet duidelijk als leeg te zien is in punt 5, fotografeer deze dan nogmaals in detail.		
10a	Berg de geheugenkaart(en) op in een klein ESD zakje 5×8cm, en plak er een SIN - sticker op. Dit zakje moet in de originele verpakking waar de RFID sticker op zit.	Bijvoorbeeld de zakjes <merk>, <type>	

10b	Maak een foto van het zakje met de SIN (sticker) geheugenkaart(en) zichtbaar er in		Als het niet mogelijk is met de Canon Powershot G5X MarkII om van het kenmerken een foto te maken. Neem dan een andere camera met scheerlicht. Vergeet niet deze foto ook in de zakenmap te plaatsen.
11	Neem foto's van eventueel beschadigde of verbroken garantiezegels en noteer deze.		
12	Fotografeer en noteer grote beschadigingen op de behuizing en eventuele verbroken garantie zegels. Grote beschadigingen zijn diepe krassen, stukken uit de behuizing, breuken in de behuizing, kapotte schermen, etc. Lichte krassen en afbladerende verf zijn beschadigingen door dagelijks gebruik. Bij twijfel fotografeer.		
13	Volg bij vochtschade de werkvoorschrift: "dt – Reinigen en conserveren van elektronica" (QOL-02364). Fotografeer eventueel verkleurde vochtindicator. Deze zit vaak in het batterijcompartiment, maar is niet altijd zichtbaar.		Bijvoorbeeld de blauwe stickers op schroefjes in BlackBerry's
14 	Alleen voor ISP/JTAG/Chip-off: Demonteer de telefoon. Als de printplaat beschadigingen heeft, neem er foto's van en noteer deze op het waarnemingsformulier. Een voorbeeld hiervan is ontbrekende microfoon en/of camera module. Wanneer een PCB - revisie nummer zichtbaar is op de PCB, fotografeer deze dan ook. Kennis over demontage staat in Afdeling\Kennis\Hardware\<TYPE APPARAAT>\Merk\Model\demontage. Doe na het demonteren de niet noodzakelijke componenten in de grote ESD zak.	Controleer voor aanvang van demonteren de ESD - maatregelen. Controleer nogmaals of sim en geheugenkaart slot leeg zijn. Als er voor een bepaald merk/model geen informatie staat in de kennis mappen, dan kan er bijvoorbeeld op www.ifixit.com, www.youtube.com of via	

FDT - Technische intake hardware

		www.google.com gezocht worden naar een disassembly of tear down van het desbetreffende merk/model.	
14 B	In sommige devices zijn meer dan één identieke relevante componenten aanwezig, bijvoorbeeld NAND-geheugen chips. Na extractie kan de originele locatie van de chips relevant zijn. Om deze componenten op de juiste plaats terug te kunnen zetten moet de originele locatie vastgelegd worden. Markeer daarom op de nog intacte PCB de identieke chips op een geschikte manier. Bijvoorbeeld met een kraspennetje, paint marker, etc. Maak daarna een foto waarop positie en markering duidelijk zichtbaar is. NB: Zorg ervoor dat een markeringsmethode wordt gekozen die niet uitgewist kan worden tijdens de extractie. Bijv: Sommige markeringen met paint markers worden opgelost in Flux Remover.		
15	Wanneer de PCB gesoldeerd of gezaagd gaat worden, demonteer dan tot op de kale PCB. Demonteer de camera uit het toestel wanneer nodig. Doe de camera in een ESD doosje en voorzie deze van een sticker CAMERA en zaaknummer en SIN.		
16	Wanneer het geheugen gesoldeerd gaat worden: Demonteer tot op de PCB. Verder moeten alle componenten die kunnen smelten van de printplaat worden verwijderd. Dit zijn het beeldscherm, stickers, camera, plastic en rubberen onderdelen, schroeven etc. Schrijf daarna met de rode paint marker (bijvoorbeeld Intrama SL150) het SIN op de printplaat, dat kan aan de voorzijde van de telefoon. Leg de printplaat op de geprepareerde ESD zak en maak een foto van beide zijde de printplaat. Print een 'stoof' sticker en plak die op de geprepareerde ESD zak. Voorzie een ESD- doosje van zaaknummer en SIN en doe die in de zakenbak. Maak één laatste foto van de PCB op de ESD zak	Labels kunnen geprint worden met de DYMO-labelprinter. Voorgeformateerde labels staan onder 'saved labels'	

FDT - Technische intake hardware

	waarop de in-stoof tijd sticker te zien is.		
17	Wanneer het SVO via JTAG onderzocht wordt, zorg dan dat de JTAG - contacten vrij zijn. Volg daarna werkvoorschrift: “dt – JTAG flasher box imaging” QoL QOL-02353		
18	Plaats na het fotograferen de foto's in 5.1.2i		
19	Geef in JIRA aan wat de vervolg stappen zijn en selecteer de volgende operator		