23

10.2.e (1)

Van: 10.2.e (8)
Verzonden: vrijdag 9 september 2011 18:19
Aan: 10.2.e (3)
Onderwerp: RE: Nieuwe onderzoeksmethode BlackBerry in zaak Poentje Castro

10.2.e (3)

dank je wel. Ik denk dat vooral de Chat en Ping berichten van 23 december 2010 ons misschien wat duidelijkheid kunnen gaan geven.

dank je wel en een goed weekend.

10.2.e (8)

On 09/09/11, 10.2.e (3) wrote:
Geachte 10.2.e (8)

Hierbij voorlopige resultaten van het onderzoek met de nieuwe onderzoeksmethode (UFED Physical Analyzer version 2.3.0.9225). Let op, het gaat hier om voorlopige resultaten, dus geldt de volgende uitsluiting:

De waarneming(en), bevinding(en) en/of conclusie(s), als vermeld in dit rapport, hebben nadrukkelijk een voorlopig karakter, waaraan geen definitieve conclusies verbonden mogen worden. Aangezien op dit moment nog niet alle onderzoeksresultaten bekend zijn, volgt - na dit voorlopig rapport - een formeel NFI-rapport (met definitieve conclusies)

De belangrijkste verschillen samengevat:
Item NFI methode UFED-PA
- toelichting

Calendar 157 201
- UFED PA methode heeft 44 items meer gevonden. NFI methode lijkt niet volledig.

Call log 1119 1202
- UFED PA methode heeft 83 items meer gevonden. NFI methode lijkt niet volledig.

Contacts 555 676
- UFED PA heeft 121 meer items gevonden. NFI methode lijkt niet volledig.

Cookies - 30
- NFI methode kan geen 'cookies' detecteren

E-mails 1516 1510
- NFI methode heeft 6 e-mails meer gevonden. De NFI methode detecteert ook zogenaamde BlackBerry 'pin-to-pin' berichten en slaat deze op als e-mail.
- De NFI methode maakt geen onderscheid tussen in- en uitgaande email
- De NFI methode kan ingepakte (compressed) berichten niet uitpakken. In dat geval staat er '' in de tekst van het bericht. De UFED methode pakt deze berichten wel uit. Zie bijvoorbeeld NFI e-mail #3 en UFED e-mail In #3.
- Er is een tijdsverschil van enkele minuten in ontvangst tijdstip van ontvangen e mail berichten. Het is nog niet onderzocht welk van de twee tijdstippen het correcte tijdstip is.

Notes - 1

- NFI methode kan geen 'notes' detecteren

SMS messages 278 278

- De NFI methode kan ingepakte (compressed) sms berichten niet uitpakken. In dat geval staat er " in de tekst van het bericht. De UFED methode pakt deze berichten wel uit. Zie bijvoorbeeld NFI sms inbox #1 en UFED sms inbox #1.
- Er is een tijdsverschil van uren in ontvangst tijdstip van ontvangen sms e mail berichten. Uit analyse van in andere zaken, waarbij tijdstippen in een sms bericht zijn vergeleken met het vermeldde ontvangst tijdstip. bleek dat de tijd die UFED aangeeft correct is.
Dit betekent dat ontvangen sms-bericht #147 op 23-12-2010 0:37:21 (UTC+0) is ontvangen en niet op 22-12-2010 14:37:17

Web historie - 76
- NFI methode kan geen 'web historie' items detecteren

Ik werk eraan om volgende week de formele rapportage hiervan af te ronden en u toe te zenden.

Vriendelijke groeten,

10.2.e (3)

Nederlands Forensisch Instituut
Digitale Technologie en Biometrie
Groep Digitale Technologie

Bezoekadres: Laan van Ypenburg 6 2497 GB Den Haag 52.044812N 4.358734E

Postadres: Postbus 24044 2490 AA Den Haag

10.2.e (3)

Route beschrijving: www.forensischinstituut.nl/Images/routebeschrijving_nfi_tcm68-92971.pdf
PGP key: http://www.holmes.nl 10.2.e (3)

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Ministerie van Veiligheid en Justitie
Nederlands Forensisch Instituut

> -----Original Message-----
> From: 10.2.e (8)
> Sent: maandag 15 augustus 2011 15:48
> To: 10.2.e (3)

> Subject: Re: Nieuwe onderzoeksmethode BlackBerry in zaak
> Poentje Castro
>
>
> Bon dia 10.2.e (3)
>
> heel graag ontvangen wij van U een aanvullend rapport met
> aanvullende onderzoeks resultaten.
>
> dank U wel ,
>
> hartelijke groet,
>
> 10.2.e (8)
>
>
> On 08/12/11, 10.2.e (3) wrote:
>
> Geachte 10.2.e (8)
>
> Sinds enkele weken biedt het programma UFED Physical
> Analyzer ondersteuning voor de analyse van gegevenskopieën
> van mobiele telefoons van het merk RIM, type BlackBerry,
> zoals die ook voorkomt in genoemd onderzoek.
>
> We hebben de gegevenskopie die al was veiliggesteld in
> genoemd onderzoek opnieuw onderzocht met dit nieuwe
> programma. Er zijn nieuwe resultaten en verbeteringen op de
> eerder gerapporteerde resultaten.
>
> Als het van belang is in het onderzoek kan ik een
> aanvullende rapportage maken met daarin opgenomen deze nieuwe
> resultaen en de verbeteringen.
>
> Ik hoor graag van u of dit gewenst is. Mocht u nog
> vragen hebben, belt u mij dan even.
>
> Vriendelijke groeten,
>
> 10.2.e (3)
>
> ---
> Nederlands Forensisch Instituut
> Digitale Technologie en Biometrie
> Groep Digitale Technologie
>
> Bezoekadres: Postadres:
> Laan van Ypenburg 6 Postbus 24044
> 2497 GB Den Haag 2490 AA Den Haag
> 52.044812N 4.358734E
>
> 10.2.e (3)
>
>
> ---
>
> Route beschrijving:
> www.forensischinstituut.nl/Images/routebeschrijving_nfi_tcm68-

> 92971.pdf
> PGP key: http://www.holmes.nl
>
> Dit bericht kan informatie bevatten die niet voor u is
> bestemd. Indien u niet de geadresseerde bent of dit bericht
> abusievelijk aan u is toegezonden, wordt u verzocht dat aan
> de afzender te melden en het bericht te verwijderen. De Staat
> aanvaardt geen aansprakelijkheid voor schade, van welke aard
> ook, die verband houdt met risico's verbonden aan het
> elektronisch verzenden van berichten.
>
> This message may contain information that is not
> intended for you. If you are not the addressee or if this
> message was sent to you by mistake, you are requested to
> inform the sender and delete the message. The State accepts
> no liability for damage of any kind resulting from the risks
> inherent in the electronic transmission of messages.
>
> Ministerie van Veiligheid en Justitie
> Nederlands Forensisch Instituut
>
>
>