

Referentie/Documentnummer: 003

Betreft: veiligstellen laptop ten behoeve van digitaal onderzoek

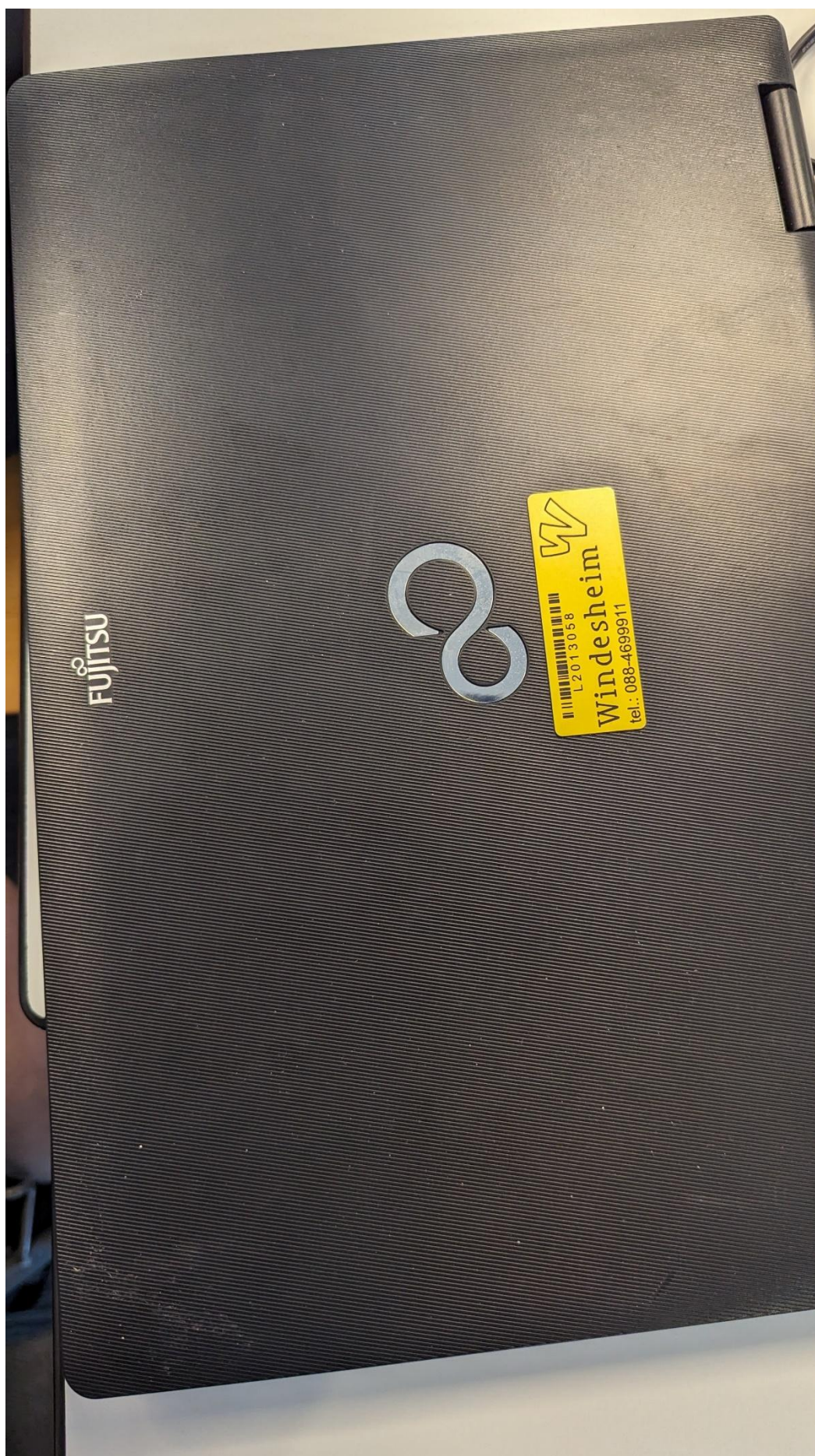
Datum: 15-5-2024

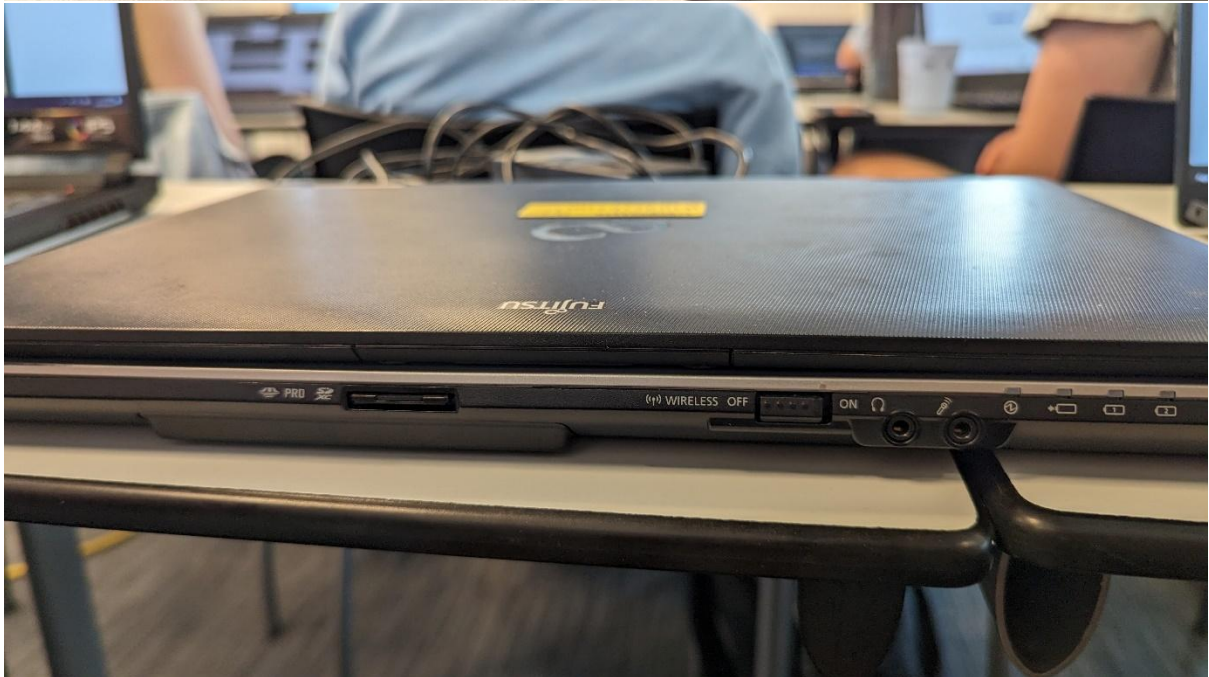
Rapporteur: [REDACTED] Ivan, [REDACTED]

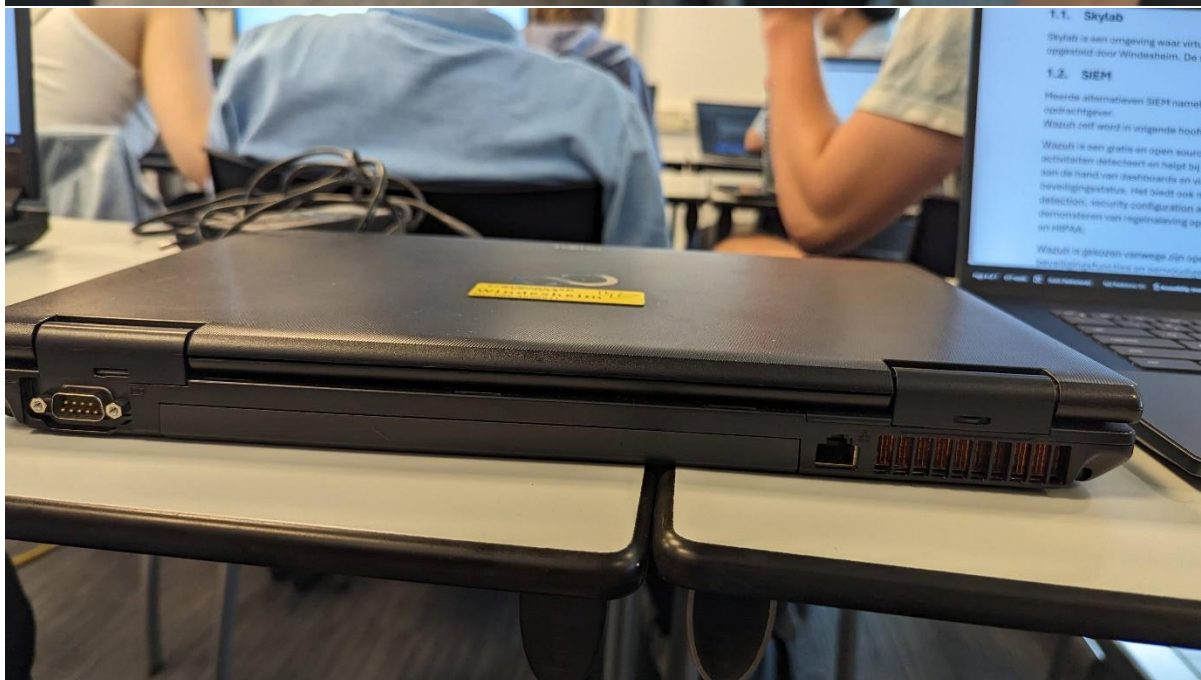
Bevindingen

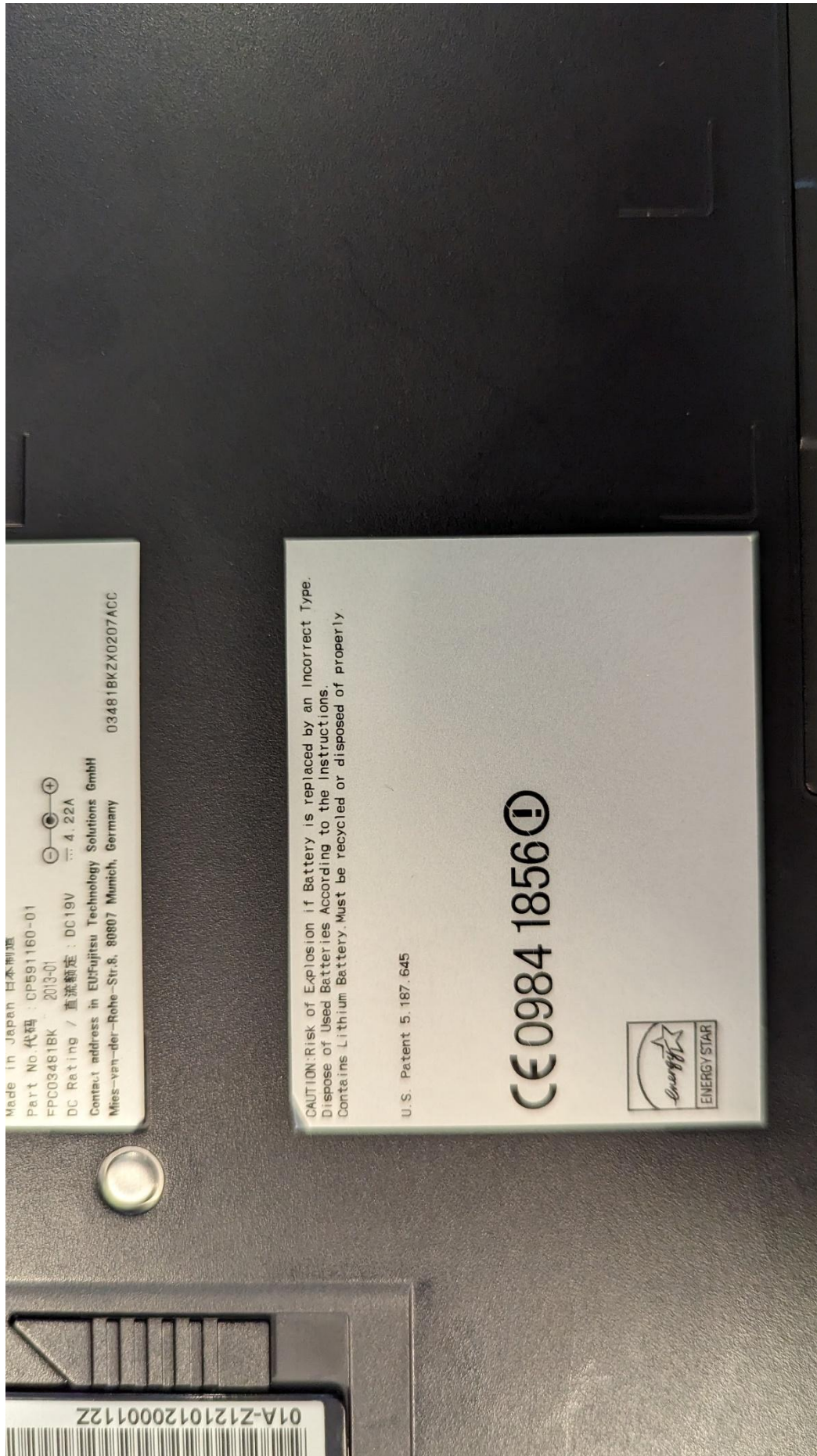
In het kader van het onderzoek zwarte laptop hebben we op 15 mei 2024 op verzoek van de leider van het onderzoek Dennis, de data van een zwarte laptop van het vermoedelijke Fujitsu merk met vermoedelijke type Livebook E-series is veiliggesteld. Met een micro SD-kaart in de laptop van vermoedelijk Kingston merk. Wij hebben gebruik gemaakt van Linux LiveOS om een image te maken zonder de laptop aan te tasten. De image van de hardeschip is HardeschijfImageAISc3.E01. de image van de micro SD-kaart is BitlockImageAISc3.E01.

De laptop is vervolgens door ons overgedragen aan de leider van het onderzoek Dennis.

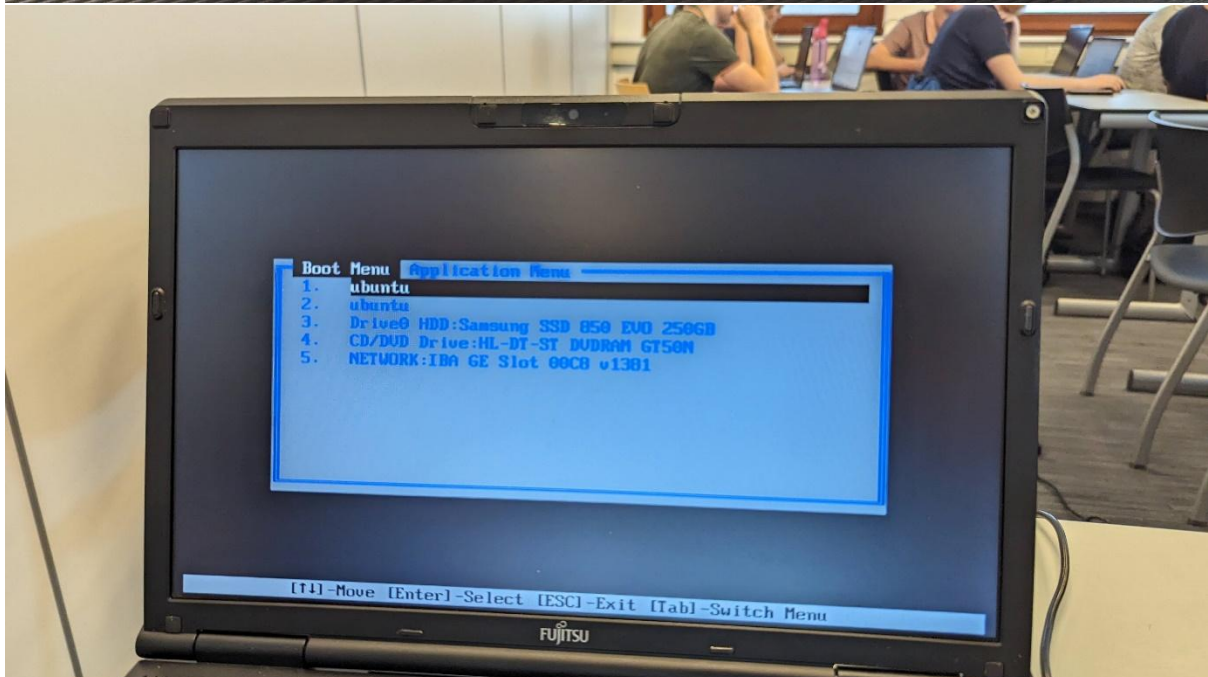
















Logging

Datum/tijd	Handeling/Observatie/Resultaat
15-5-2024 12:48	Laptop van Anton de Bok gekregen van Dennis
15-5-2024 12:49	Foto's gemaakt van buitenkant
15-5-2024 12:50	Merk: vermoedelijk Fujitsu, type: vermoedelijk Livebook E series, kleur: zwart, opslagcapaciteit: vermoedelijk 256GB, serienummer: DSCN503355
15-5-2024 12:55	CD schijf lezer eruit gehaald, geen CD erin
15-5-2024 13:00	SD-kaart eruit gehaald en foto's gemaakt
15-5-2024 13:01	SD-kaart merk: vermoedelijk Kingston micro SD adapter, opslagcapaciteit: vermoedelijk 16GB
15-5-2024 13:11	Laptop geopend
15-5-2024 13:12	Aan knop gedrukt, deed niks
15-5-2024 13:12	Stroom aangesloten
15-5-2024 13:13	Laptop opgestart met f12 ingedrukt houden
15-5-2024 13:14	Boot menu geopend
15-5-2024 13:15	USB stick met Live OS Kali versie: 2024.1 ingeplugd
15-5-2024 13:15	Laptop opnieuw opgestart
15-5-2024 13:16	Laptop gestart en boot menu geopend
15-5-2024 13:17	Laptop gestart via de Live OS
15-5-2024 13:18	Kali linux forensic mode met succes opgestart
15-5-2024 13:21	In Kali met Gparted de schijven verkend
15-5-2024 13:22	Machine shutdown gedaan in kali Linux
15-5-2024 13:23	Laptopstroom verwijderd en meegenomen door Ben
16-5-2024 11:05	Laptop weer geboot op Kali Live OS & externe harde schijf aangesloten
16-5-2024 11:15	Laptop hardware geprint in terminal met cat /proc/<hardware>info, Bevat ~39 GB RAM, een Intel Core i5-3210M CPU. In Gparted alle devices verkend, bevat ~250GB Harde Schijf op /dev/sda en ~15GB data drager op /dev/mmcblk0. De batterij is volgens Kali Fujitsu CP293551-02. De 15GB data drager is gebitlocked.
16-5-2024 11:55	Begonnen met imageren van de ~15GB data drager mmcblk0 met guymager Expert Witness Format optie en op externe harde schijf geplaatst met de naam BitlockImageA1Sc3.
16-5-2024 12:01	Imageren is klaar, externe harde schijf verwijderd en image gekopieerd naar Linux laptop van onderzoeker Tim met read-only mount.
16-5-2024 12:27	Begonnen met imageren van de ~250GB harde schijf /dev/sda met guymager Expert Witness Format optie en op externe harde schijf geplaatst met de naam HardeschijfImageA1Sc3.
16-5-2024 12:29	Laptop afgesloten met shutdown commando van Kali
16-5-2024 13:35	Laptop afgedragen aan leider van onderzoek Dennis