Chain of Custody Form

**Case Number**: 78631 **Evidence Number:** 001

**Custodian Name:** Amatullah Vakhariya **Form Completed By**: Jacinth Daniel Moses

**Type of Incident:** Data Theft **Date and Time of Incident:** 08/27/2023 10:11PM

**Location of Incident:** 3507, Latifa Tower, Dubai, UAE

**Section A: Forensic Investigator’s Information**

| Name | Jacinth Daniel Moses | Contact Information | +971505873197 |
| --- | --- | --- | --- |
| Organization | Plus971 Cyber Security | Signature |  |
| Organization’s Location | 3507, Latifa Tower, Dubai, UAE | | |

**Section B: Evidence Details**

| Item Description | Yasir Umer HP ENVY laptop 1TB,Silver Color, Size: 15.6 inches | | |
| --- | --- | --- | --- |
| Location Of Discovery | Plus971 Cyber Security | | |
| Evidence Type | Laptop | Model/Manufacturer | HP ENVY |
| Evidence ID/Tag Number | 001 | Capacity | 1TB |
| Evidence State | **On/Logged**  | On/Loggedoff | Off | Other | | |
| Serial/ID Number | 5CD4364YDG | Date/Time/Timezone Of Recovery | 8/28/2023 12:34 PM GMT+4 |
| Front Picture(s) |  | | |
| Back Picture(s) |  | | |

**Section C: Acquisition Information**

| IMAGE DETAILS | | | |
| --- | --- | --- | --- |
| Image Name | YASIR\_UMER\_HP\_LAPTOP\_1TB\_CASE\_73156.E01 | Destination Drive S/N | NABP6MLX |
| Tool Name | FTK Imager | Version | 4.7.1.2 |
| Image Format | E01 | Acquisition Type/ Method | Logical extraction/ Live forensics |
| MD5 Hash | fdb85ed46d3100794c9bb2990a585dda | Acquisition Start Time | Mon Aug 28 13:29:30 2023 |
| SHA1 Hash | ffe951df30a1c97f113649e0fedc665d748b472d | Acquisition End Time | Mon Aug 28 16:30:30 2023 |
| Hash Validated (Yes/No) | Yes | Acquisition Location | Plus971 Cyber Security |
| MEMORY DUMP DETAILS | | | |
| Memory Dump File Name | memcapture.ad1 | Destination Drive S/N | NABP6MLX |
| Tool Name | FTK Imager | Version | 4.7.1.2 |
| Image Format | AD1 | Acquisition Type/ Method | Memory dump |
| MD5 Hash | f88b8b39c5d5a3102b1b6858a9069aee | Acquisition Start Time | Mon Aug 28 13:13:50 2023 |
| SHA1 Hash | 6c08cb5ac7d79fda8d53e5362f44549e2e96c296 | Acquisition End Time | Mon Aug 28 13:26:36 2023 |
| Hash Validated (Yes/No) | Yes | Acquisition Location | Plus971 Cyber Security |

**Section D: Target Drive Description**

| Type Of Drive | HDD | Size | 2TB |
| --- | --- | --- | --- |
| Model/Manufacturer | SEAGATE | Target Drive Tag | 002 |
| Serial Number | NABP6MLX | | |
| Front Picture(s) |  | | |
| Back Picture(s) |  | | |

**Section E: Forensic Analyst Information**

| Name | Pallavi Krishnan | Contact Information | +971502464791 |
| --- | --- | --- | --- |
| Organization | Plus971 Cyber Security | Signature |  |

**Section F: Chain Of Custody Video Recording log**

| File Name | Start Timestamp | End Timestamp | Purpose |
| --- | --- | --- | --- |
| IMG\_7730.MOV | 8/28/2023 1:08:45 pm | 8/28/2023 1:14:40 pm | FTK memory and logical acquisition |
| 20230828\_132714.mp4 | 8/28/2023 1:27:25 pm | 8/28/2023 1:29:44 pm | Memory Dump completed |
| IMG\_7731.MOV | 8/28/2023 3:48:09 pm | 8/28/2023 3:48:39 pm | Collection of evidence serial ID Number |
| IMG\_7736.MOV | 8/28/2023 4:31:28 pm | 8/28/2023 4:31:42 pm | FTK image Summary |
| 20230828\_175223.mp4 | 8/28/2023 5:52:32 pm | 8/28/2023 5:53:48 pm | Starting FTK image verification |

**Section G: Chain Of Custody Log**

| Date/Time | Received From | Received By | Purpose | Location | Signature |
| --- | --- | --- | --- | --- | --- |
| 8/28/2023  12:34pm | Amatullah | Daniel | Forensic Processing | Plus971 Cyber Security |  |
| 8/30/2023  12:09pm | Daniel | Pallavi | Forensic Analysis | Plus971 Cyber Security |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Sealed: No

Seal Number/Id: N.A

Additional Notes/Comments:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

I certify that the information provided above is accurate and complete to the best of my knowledge.

Investigator's Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: 8/30/2023