

DME Analytical Notes

Case Information

FS Lab #	
Forensic Scientist Name	
Court Ordered?	
Analysis Type	
Agency Case #	
Offense Date	
Six (6) Month Date/Time Filter (ET)	N/A
Examination Started	
Examination Completed	

Appendices

#	Name	Description
1	Appendix 1	Contains pictures of equipment settings and/or equipment output.
2		
3		
4		
5		

Examination Results (ER)

#	Item #(s)	Name	Description
1			
2			
3			
4			
5			

Examination Results Preliminary Review

#	Date	Reviewer Name	Status	Notes
1				
2				
3				
4				
5				

DME Analytical Notes

Container Description

Submission #	Container #	Container Type	Seal Upgraded?	Date Opened	Item #(s) in Container	Notes

Item Description

Item #	Agency Item #	Agency Description	DFS Description	Type	Manufacturer	Model	Unique ID(s)	Sub-Item #(s)	Area of Interest (Aoi)	Status	Notes

VIRGINIA
 DEPARTMENT
 OF
 FORENSIC SCIENCE

DME Analytical Notes

Equipment Utilized (EU)

#	Equipment	Version	Notes
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

COPYRIGHT © 2022

VIRGINIA
DEPARTMENT
OF
FORENSIC SCIENCE

DME Analytical Notes

Initial Examination (IE) - Analog Storage Device

Item #	Onboard Write-Protection	Recording Capacity	Record Mode	Quad?	Multiplexed/Switched?	Notes

COPYRIGHT © 20**22**

VIRGINIA
DEPARTMENT
OF
FORENSIC SCIENCE

DME Analytical Notes

Initial Examination (IE) - Computer Device

Item #			
EU			

Firmware / Interface

Access Method			
Version			
System Clock Setting			
System Date/Time (UTC)			
System Time Zone			
Current Date/Time (UTC)			
Time Difference (hh:mm:ss)	N/A	N/A	N/A
System Settings			
Boot Sequence			
Security Measures			
Logs Present?			
Overwrite – Status/Schedule			
Export Options			
Notes			

Item #			
EU			

Firmware / Interface

Access Method			
Version			
System Clock Setting			
System Date/Time (UTC)			
System Time Zone			
Current Date/Time (UTC)			
Time Difference (hh:mm:ss)	N/A	N/A	N/A
System Settings			
Boot Sequence			
Security Measures			
Logs Present?			
Overwrite – Status/Schedule			
Export Options			
Notes			

DME Analytical Notes

Initial Examination (IE) - Mobile Device

Item #			
EU			
Service Provider (Carrier)			
MDN / MSISDN			
(U)ICC?			
Expansion Card?			
Security Measures			
Isolation Method(s)			
Operating System (OS)			
OS Installation/Reset Date/Time (UTC)			
System Clock Setting			
System Date/Time (UTC)			
System Time Zone			
Current Date/Time (UTC)			
Time Difference (hh:mm:ss)	N/A	N/A	N/A
System Settings			
Device Profiles / User Accounts			
Activity Timeframe			
Notes			

Item #			
EU			
Service Provider (Carrier)			
MDN / MSISDN			
(U)ICC?			
Expansion Card?			
Security Measures			
Isolation Method(s)			
Operating System (OS)			
OS Installation/Reset Date/Time (UTC)			
System Clock Setting			
System Date/Time (UTC)			
System Time Zone			
Current Date/Time (UTC)			
Time Difference (hh:mm:ss)	N/A	N/A	N/A
System Settings			
Device Profiles / User Accounts			
Activity Timeframe			
Notes			

DME Analytical Notes

Initial Examination (IE) - Digital Storage Device

Item #	EU	Interface	Form Factor	Storage Capacity (Listed / Actual)	# of Partitions / Sessions	Notes

Analyzed Partitions / Sessions / Volumes

Item #	EU	Interface	Form Factor	Storage Capacity (Listed / Actual)	# of Partitions / Sessions	Notes
Partition Session #						
Partition Session Creation Date/Time (UTC)						
Volume						
Size (Bytes / Sectors)						
Label						
Bootable?						
Security Measures						
File System						
Operating System (OS)						
OS Installation Date/Time (UTC)						
System Time Zone						
User Accounts						
Data Backups						
Activity Timeframe						
Notes						

Item #	EU	Interface	Form Factor	Storage Capacity (Listed / Actual)	# of Partitions / Sessions	Notes
Partition Session #						
Partition Session Creation Date/Time (UTC)						
Volume						
Size (Bytes / Sectors)						
Label						
Bootable?						
Security Measures						
File System						
Operating System (OS)						
OS Installation Date/Time (UTC)						
System Time Zone						
User Accounts						
Data Backups						
Activity Timeframe						
Notes						

DME Analytical Notes

Data Acquisition

#	Item #	EU	Type	Evidence Source?	ER#	Acquisition Date	Acquisition File Name(s)	Hash Value	Verified?	Retained?	Notes
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											

COPYRIGHT © 2022

VIRGINIA
DEPARTMENT
OF
FORENSIC SCIENCE

DME Analytical Notes

Data Analysis

#	Item #(s)	EU	Category / Type	Source	Source Count (E)	Parsed Count (E)	Parsed Count (PE)	Parsed Count (Vir/Unk)	Excluded Count	Results Count Unique (U)	Results Count Duplicates (D)	Results Count Total	ER#	Notes
1												N/A		
2												N/A		
3												N/A		
4												N/A		
5												N/A		
6												N/A		
7												N/A		
8												N/A		
9												N/A		
10												N/A		
11												N/A		
12												N/A		
13												N/A		
14												N/A		
15												N/A		
16												N/A		
17												N/A		
18												N/A		
19												N/A		
20												N/A		
21												N/A		
22												N/A		
23												N/A		
24												N/A		
25												N/A		

DME Analytical Notes

Video Analysis

Item #			
EU			
Original Recording Name			
Derivative Name (N/A)			
Video Codec (FourCC)			
Proprietary Player			
Pixel Dimensions (Width)			
Pixel Dimensions (Height)			
Average Frames Per Second (FPS)			
Duration (hh:mm:ss.ms)			
Frame Count (Calculated)	N/A	N/A	N/A
Frame Count (Other)			
Color?			
Black & White?			
Infrared?			
Number of Cameras			
Audio Present?			
Audio Codec			
Duration (hh:mm:ss.ms)			
Number of Channels			
Sampling Rate (Hz)			
Notes			

Item #			
EU			
Original Recording Name			
Derivative Name (N/A)			
Video Codec (FourCC)			
Proprietary Player			
Pixel Dimensions (Width)			
Pixel Dimensions (Height)			
Average Frames Per Second (FPS)			
Duration (hh:mm:ss.ms)			
Frame Count (Calculated)	N/A	N/A	N/A
Frame Count (Other)			
Color?			
Black & White?			
Infrared?			
Number of Cameras			
Audio Present?			
Audio Codec			
Duration (hh:mm:ss.ms)			

DME Analytical Notes

General Analysis

#	Item #(s)	Notes
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		COPYRIGHT © 2022
11		
12		
13		
14		VIRGINIA
15		DEPARTMENT
16		OF
17		
18		
19		
20		FORENSIC SCIENCE

DME Analytical Notes

Data Authentication

		Notes
Item #		
EU		
File Name		
File Path		
Duplicate Status		
Duplicate Relationship Group		
Type Description		
Size (Bytes)		
Created (ET)		
Modified (ET)		
Accessed (ET)		
Record Changed (ET)		
Other Timestamp (ET)		
Additional Metadata		
Source Device Settings		
Editing Applications / Functions		
File Naming Convention		
File Path Analysis		
Duplicate Analysis		
File System Timestamps Analysis		
Internal Timestamps Analysis		
Metadata Analysis		
File Structure Analysis		
Track Duration Analysis		
Pixel Dimensions & DAR Analysis		
Frame Analysis		
GOP Analysis		
Jump Cuts & A/V Synchronization Analysis		
Critical Listening / Observation		
Other Analysis		

COPYRIGHT © 2022
 VIRGINIA
 DEPARTMENT
 OF
 FORENSIC SCIENCE

		Notes
Item #		
EU		
File Name		
File Path		
Duplicate Status		
Duplicate Relationship Group		
Type Description		
Size (Bytes)		
Created (ET)		

DME Analytical Notes

Data Authentication

Modified (ET)		
Accessed (ET)		
Record Changed (ET)		
Other Timestamp (ET)		
Additional Metadata		
Source Device Settings		
Editing Applications / Functions		
File Naming Convention		
File Path Analysis		
Duplicate Analysis		
File System Timestamps Analysis		
Internal Timestamps Analysis		
Metadata Analysis		
File Structure Analysis		
Track Duration Analysis		
Pixel Dimensions & DAR Analysis		
Frame Analysis		
GOP Analysis		
Jump Cuts & A/V Synchronization Analysis		
Critical Listening / Observation		
Other Analysis		

COPYRIGHT © 2022
VIRGINIA
DEPARTMENT
OF
FORENSIC SCIENCE

DME Analytical Notes

Data Authentication

#	Item #	Alt	File Name	File Path	Duplicate Status	Duplicate Relationship Group	Type Description	Size (Bytes)	Created (DT)	Modified (DT)	Accessed (DT)	Record Changed (DT)	Other Timestamp (DT)	Additional Metadata	Editing Application / Function	File Naming Convention	File Path Analysis	Duplicate Analysis	File System Timestamps Analysis	Internal Timestamps Analysis	Metadata Analysis	File Structure Analysis	Track Duration Analysis	Pixel Dimensions & DMR Analysis	Frame Analysis	GOP Analysis	Jump Cuts & JVI Synchronization Analysis	Critical Listing / Observation	Other Analysis	
1																														
2																														
3																														
4																														
5																														

COPYRIGHT © 2022

VIRGINIA
DEPARTMENT
OF
FORENSIC SCIENCE

DME Analytical Notes

Communications

#	Date	Description
1		
2		
3		
4		
5		

COPYRIGHT © 2022

VIRGINIA
DEPARTMENT
OF
FORENSIC SCIENCE

DME Analytical Notes

Examination & Analysis Complete

Examination Results Media	Description	EU
Archive Type		
Archive Name		N/A
Password		N/A
Source/Archive CRC32 Value		
Archive Hash Value		
Production Method		
Production Date		N/A
Production Verification Hash Value		
Return Method	Returned w/in a [package] [w/in / attached to] Container #	N/A
Notes		N/A

Evidence Sources Media	Description	EU
Designation	DME[#]	N/A
Archive Type		
Archive Name		N/A
Password		N/A
Source/Archive CRC32 Value		
Archive Hash Value		
Production Method		
Production Date		N/A
Production Verification Hash Value		
Return Method	Returned w/in a [package] [as / w/in / attached to] Container #	N/A
Notes		N/A

Electronic Case File [ECF] Media	Description	EU
Archive Type		
Archive Name		N/A
Password		N/A
Source/Archive CRC32 Value		
Archive Hash Value		
Production Method		
Production Date		N/A
Production Verification Hash Value		
Notes		N/A

End of Notes

DME Analytical Notes

Audit Log

Date	User	Worksheet	Cell	New Value	Previous Value

COPYRIGHT © 2022

VIRGINIA
DEPARTMENT
OF
FORENSIC SCIENCE

DME Analytical Notes

#	Analysis Type	Preliminary Review Status	Container Type	Item Type	Item Status	Equipment	Onboard Write Protection	Interface	Form Factor	Yes / No	Acquisition Type	Derivative Name	Duplicate Status	Data Authentication	Archive Type	Production Method
1	Broad	Approved	None	Blu-ray Disc (BD)	Examined	7-Zip (7Z)	Tabin	Firewire	1.1	Yes	Clone	Derivative Name (Transcoded)	Primary	Expected	7-Zip (7Z) archive	Burned archive and hash file to Blu-ray disc (BD)
2	Extraction Only	Disapproved	SBB	Compact Disc (CD)	Reviewed	Acrobat Pro (AcP)	TAB-Out	SP	2.0	No	File System	Derivative Name (Rewrapped)	React	Not Expected	7-Zip (7Z) split archive	Burned archive and hash file to compact disc (CD)
3	Normal		SBBP	Desktop Computer	Analyzed		Tab Removed by Examiner	JTAG	3.0	N/A	Logical	Derivative Name (Other)	Near		Self-extracting 7-Zip (7Z) archive	Burned archive and hash file to digital versatile disc (DVD)
4			SR	Digital Camera	N/A	Adobe Bridge (AB)	N/A	RAW	2.1	Other	Physical	Derivative Name (N/A)	Visual	Other	Self-extracting 7-Zip (7Z) split archive	Burned archive and hash file to dual-layer Blu-ray disc (BD-DL)
5			SEN	Digital Video Recorder (DVR)	Other	Android Studio / SDK	Other	PCIA (IDE)	1.5*	Unknown	N/A	N/A	Unknown	Unknown	Encrypted and password-protected, 7-Zip (7Z) archive	Burned archive and hash file to dual-layer digital versatile disc (DVD-DL)
6			SFB	Digital Video/Versatile Disc (DVD)	Other	Acrobat Reader (AR)	Unknown	PCIe	2.5*	Other	Other	Unknown	Unknown	Unknown	Encrypted and password-protected, 7-Zip (7Z) split archive	Burned archive and hash file to triple-layer Blu-ray disc (BD-TL [RL])
7			SPB	Feature Phone	Autopsy (AT)			SAS	3.5*	Other	Unknown	Unknown	Unknown	Unknown	Encrypted and password-protected, self-extracting, 7-Zip (7Z) archive	Electronic File Transfer (EFT)
8			SWB	Flash Drive	Avast (AV)			SATA	3.6*	Other	Unknown	Unknown	Unknown	Unknown	Encrypted and password-protected, self-extracting, 7-Zip (7Z) split archive	Wrote archive and hash file to hard disk drive (HDD)
9			SWEN	Global Positioning System (GPS)	Avast! F-Protect (AF)			SCSI	M.2						ZIP archive	Wrote archive and hash file to network-attached storage (NAS)
10			SWPB	Hard Disk Drive (HDD)	Amped FIVE (AF)			SATA	M.2						ZIP split archive	No Electronic Case File (ECF) archived
11			SVN	Laptop Computer	Armitage (AM)			SATA	M.2						ZIP archive	No Examination Results produced
12			N/A	Magnetic Card Skimmer	Armitage (AM)			SATA	M.2						Encrypted and password-protected, ZIP archive	No Evidence Sources produced
13			Other	Memory Card	Bitwark (BW)			USB	Micro						Encrypted and password-protected, ZIP split archive	No Evidence Sources produced
14			Unknown	Media/Video Player	CamStudio (CT)			USB	Micro						Encrypted and password-protected, ZIP split archive	No Evidence Sources produced
15				Network-Attached Storage (NAS)	CellScribe Physical Analyzer (PA)			USB	Micro						Encrypted and password-protected, ZIP split archive	No Evidence Sources produced
16				Network Video Recorder (NVR)	CellScribe Premium (CPM)			Other	Other	Unknown					Other	N/A
17			Protout	Server	CellScribe Reader (CR)			Other	Other	Unknown					Other	Other
18			Server		CellScribe Digital Collector (CDC)			Other	Other	Unknown						
19				Smartphone	CellScribe UPD Downloader (UDL)											
20				Solid-State Drive (SSD)	CellScribe UPD-ARC (UARC)											
21				Tablet	CellScribe UPD-Touch 2 (UT2)											
22				Universal / Integrated Circuit Card (UICC)	CellScribe UPD User Lock Code Recovery Tool (ULCRT)											
23				Video Camera	CH341A USB Programmer (CUP)											
24				Video Game Console	Chip-Off (CO)											
25					Clear-It! PhotoShop Filter Plugins (CID)											
26					DMG											
27					CyberChef (CC)											
28					DBeecher Community Edition (DBCE)											
29					DB Brower for SQLite (DB4S)											
30					DCable (DC)											
31					DC Power Supply (DPS)											
32					DD (DD)											
33					Disk Library (DL)											
34					DME-COMPUTER-1 (DC1)											
35					DME-COMPUTER-2 (DC2)											
36					DME-COMPUTER-3 (DC3)											
37					DME-COMPUTER-4 (DC4)											
38					DME-COMPUTER-5 (DC5)											
39					DME-COMPUTER-6 (DC6)											
40					DME-COMPUTER-7 (DC7)											
41					DME-COMPUTER-8 (DC8)											
42					DME-MOBILE-1 (DM1)											
43					DME-MOBILE-2 (DM2)											
44					DME-MOBILE-3 (DM3)											
45					DVR Exammer (DE)											
46					EnCase Forensic (EF)											
47					EnCase (E3)											
48					ESP000Recovery (ESP0V)											
49					Evidence Sync (ES)											
50					Evtkunter (EK)											
51					EvtkunterView (EDV)											
52					Exploit (ET)											
53					Fmpeg											
54					Flpylog											
55					Flrprobe											
56					FinalMobile Forensic (FMMF)											
57					Fluke Digital Multimeter (FDM)											
58					Forensic Toolkit Imager (FTI-8)											
59					Forensic Toolkit Imager Lite (FTX-IL)											
60					Forensic Toolkit Registry Viewer (FTKRV)											
61					Forensic Unlocker v3 (FUD)											
62					FreeCommander XE (FC)											
63					FunToolGold (FG)											
64					Google Chrome (GC)											
65					Google Earth (GE)											
66					GrayKey (GK)											
67					Griffeye Analyser (GA)											
68					Gspot (GT)											
69					GuardDns (GD)											
70					HashCheck (HC)											
71					HashMyFiles (HMf)											
72					hex2x (HX)											
73					Hyper-IT (HY)											
74					imgBurn (IB)											
75					In-System Programming (ISP)											
76					Intensity Shuttle (IS)											
77					Intelligence (IV)											
78					Iron Python (IP)											
79					Isobuster (IS)											
80					Jabba the Ripper (JR)											
81					JTAG (JTAG)											
82					KAPE (KAP)											
83					Log Parser (LP)											
84					MediaConch (MC)											
85					MediaInfo (MI)											
86					MFT Hex Converter (MHNC)											
87					MFT Stampede (MS)											
88					Microsoft Access (MA)											
89					Microsoft Excel (ME)											
90					Media Express (MX)											
91					Microsoft Word (MW)											
92					Memento (ME)											
93					Mozilla Firefox (MF)											
94					mPlayer (MP)											
95					NCMEC ESP Client (NCC)											
96					NetAnalysis (NA)											
97					Notepad											
98					Notepad++ (NPP)											
99					Nxfs Workstation (NX)											
100					Oxygen Forensic Detective (OFD)											
101					Pabsoft (PA)											
102					Paparazzi Kit Forensic (PKF)											
103					PerzHound (PH)											
104					PhotoShop (PS)											
105					PuTTY (PU)											
106					Premiere Pro (PP)											
107					Promax MICRO M3 MF 70 (PMM)											
108					Python (PY)											
109					QuickTime (QT)											
110					Registry Explorer (RE)											
111					Registry Mirror (RM)											
112					RFF Box / J											

DME Analytical Notes

#	Analysis Type	Preliminary Review Status	Container Type	Item Type	Item Status	Equipment	Onboard Write-Protection	Interface	Form Factor	Yes / No	Acquisition Type	Derivative Name	Duplicate Status	Data Authentication	Archive Type	Production Method
119						The Sleuth Kit (TK)										
120						Timeline Explorer (TLE)										
121						Timeline (TL)										
122						Ultrabay Forensic Card Reader (UFCR)										
123						Ultrabay II Forensic Bridge (UFB)										
124						UP-828 Programmer (UP-828)										
125						USB View (UV)										
126						USBReview (UR)										
127						VideoFocus Pro (VFP)										
128						VirusTotal (VT)										
129						VLC Media Player (VLC)										
130						VMWare (VM)										
131						Volatility (VI)										
132						Wget										
133						Windows Command Processor/Prompt (WCP)										
134						Windows [FAT] Explorer (FE)										
135						Windows Media Player (WMP)										
136						Windows PowerShell (PS)										
137						Windows Registry USB WriteProtect (WRUB)										
138						Windows Subsystem for Linux (WSL) - Ubuntu Linux (UL)										
139						Windows Subsystem for Linux (WSL) - Kali Linux (KL)										
140						WinPE (WPE)										
141						WinHex (WH)										
142						Wireshark (WS)										
143						YAFFS / XACT / XRV / XACT)										
144						0-Range Forensics (ORF)										
145						YAFFS (YF)										
146						YAT - Yet Another Terminal (YAT)										
147						ZSK Pro Box / ZSK Easy IIAG Suite (ZSK)										

COPYRIGHT © 2022

VIRGINIA
DEPARTMENT
OF
FORENSIC SCIENCE