Dead Man's Switch: Forensic Autopsy of the Nintendo Switch

By:
Frederick Barr-Smith, Danny Rigby, Sash Rigby, Tom Farrant, Benjamin Leonard-Lagarde and Frederick Sibley-Calder

From the proceedings of
The Digital Forensic Research Conference
DFRWS EU 2021
March 29 - April 1, 2021

Digital Crime Scene:
Dead Man's Switch: Forensic Autopsy of the Nintendo Switch

Frederick Barr-Smith, Thomas Farrant, Benjamin Leonard-Lagarde, Danny Rigby, Sash Rigby and Frederick Sibley-Calder

About Us

- Technical Security Consulting for Telecoms, Finance and FTSE100
  - Digital Forensics
  - Offensive Security
  - Web & Mobile Application Security
  - Infrastructure Security
  - Penetration Testing - CHECK testing
  - Red Teaming

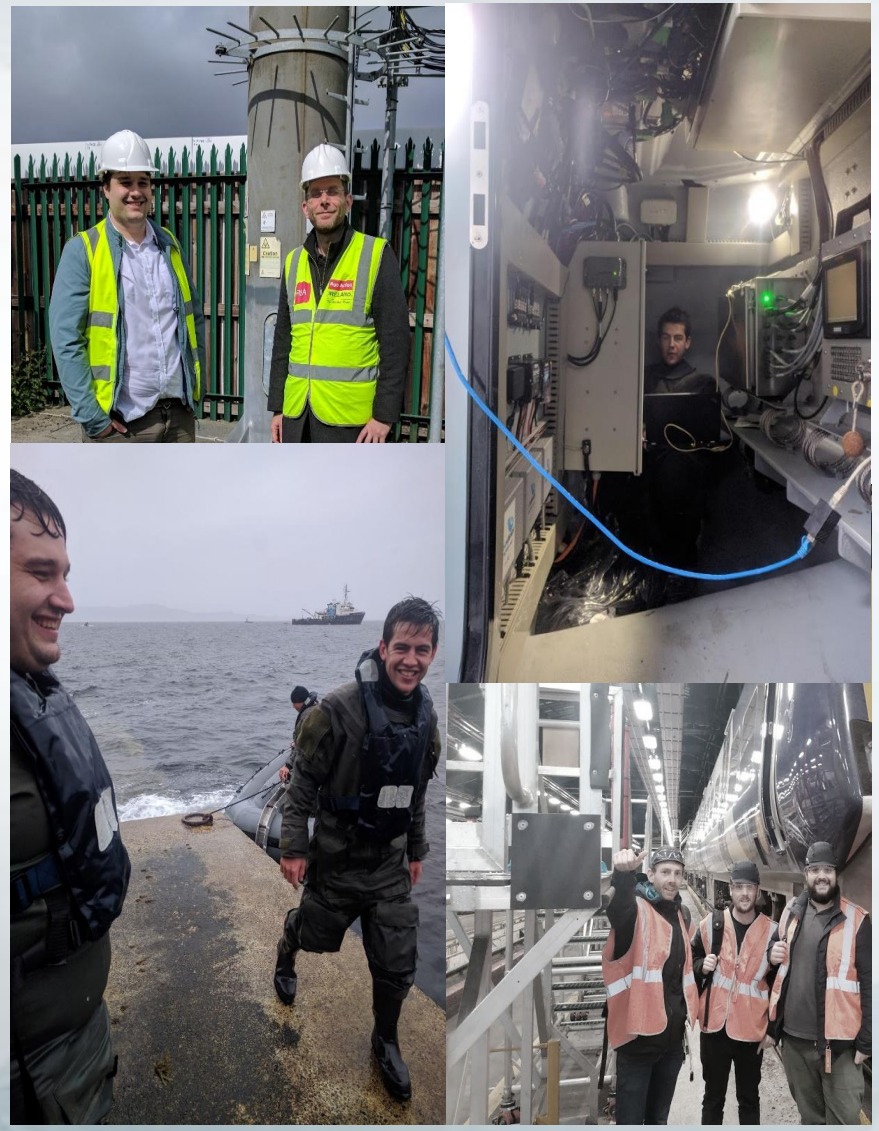
[dstl]

UNIVERSITY OF OXFORD

modux

About Us

- Bespoke Research and Development
  - Digital Forensics
  - Simulation and Augmented Reality
  - Augmented Reality for Medical Emergency Response Training
  - Critical Infrastructure Security (Rail/Telecoms)
  - Automated Maritime USV



[dstl]

UNIVERSITY OF OXFORD

modux

Why the Nintendo Switch?

- Rapidly growing market
- Portable!

[dstl]

UNIVERSITY OF OXFORD

modux

Why the Nintendo Switch?

NCA
National Crime Agency

Intelligence Assessment

Pathways Into Cyber Crime

Work with the video gaming industry to deliver Prevent activity: It is clear that the majority of cyber criminals, or those on the periphery of cyber crime, are also online gamers (as the cease & desist analysis shows, many got into computing and technology via their interest in gaming). This, of course, does not mean all gamers are cyber criminals. GameTrack estimate that 40% of the UK population play video games[10]. Current statistics concerning the US

[dstl]

UNIVERSITY OF OXFORD

modux

Autopsy Modules - Open Source

Nintendo-Switch-Forensics

Autopsy folder contains the following Autopsy ingest modules:

Module	Purpose
ingest_connected_displays	all recently connected displays
ingest_game_history	recent game history
ingest_crash_dumps	last 50 crash dumps
ingest_device_accounts	all user accounts saved to device
ingest_gamesaves	all saved games
ingest_last_boot	last boot time of device
ingest_mp_user_history	last 300 users played with and game played
ingest_power_states	device power history
ingest_screenshots	all saved recordings and screenshots
ingest_wifi	details of all WiFi networks recently connected to

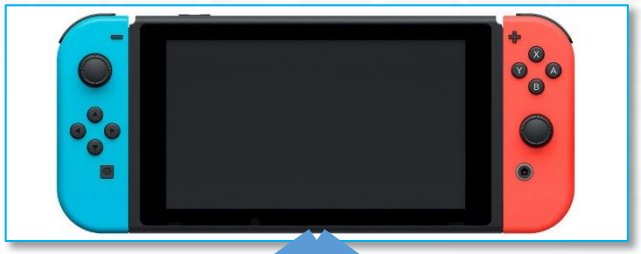
memory-dump-utils folder contains utilities to aid in performing Switch memory dumps

[dstl]

UNIVERSITY OF OXFORD

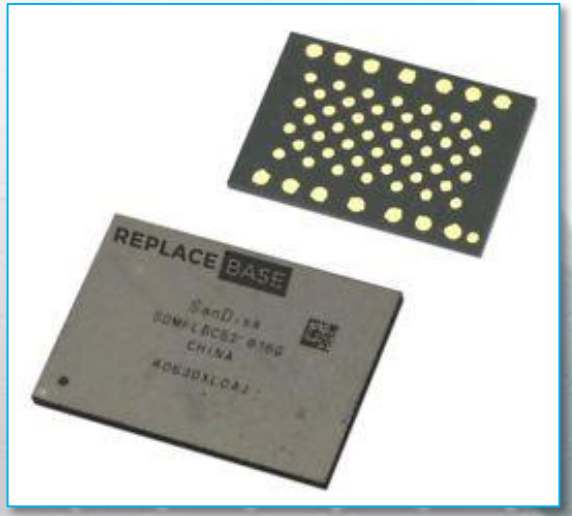
modux

Where is the data?



Onboard NAND Flash Memory

Removable SD Card

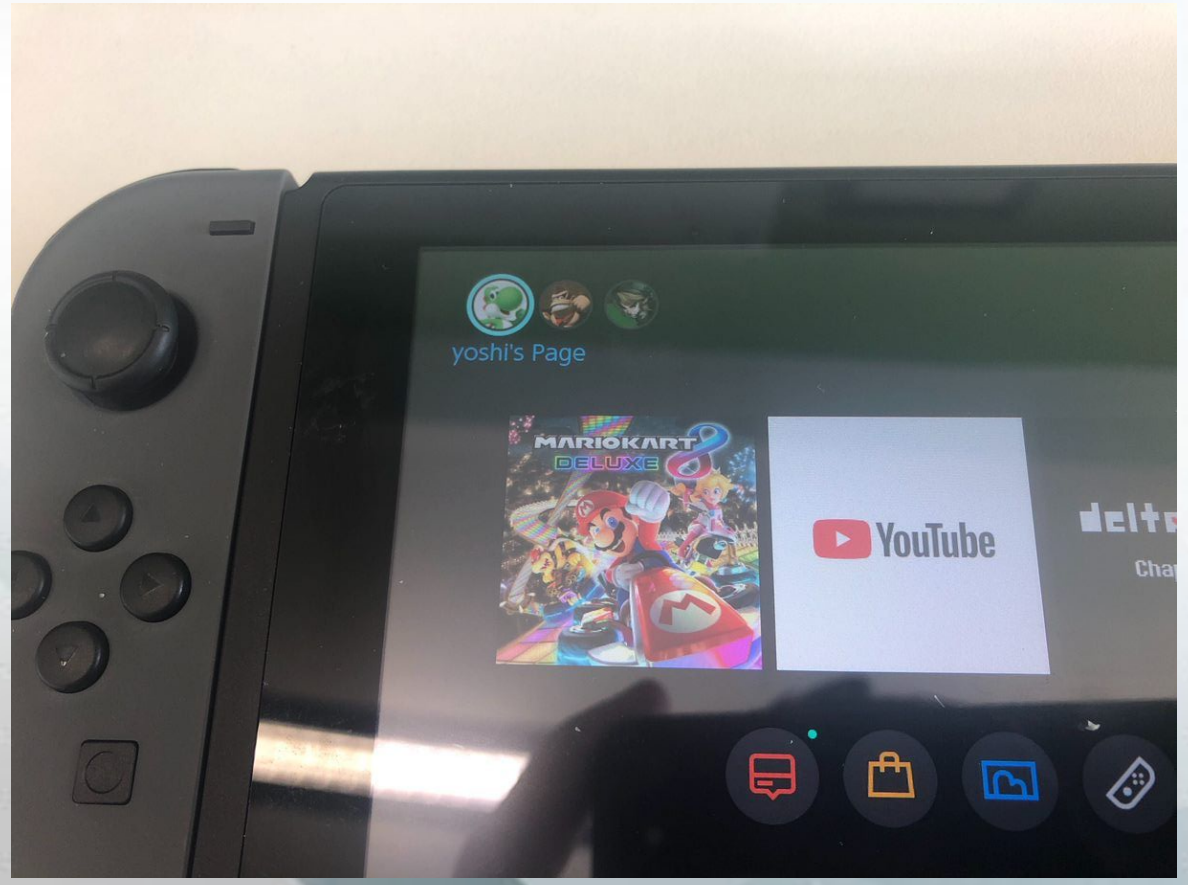


[dstl]

UNIVERSITY OF OXFORD

modux

Creation of Test Data

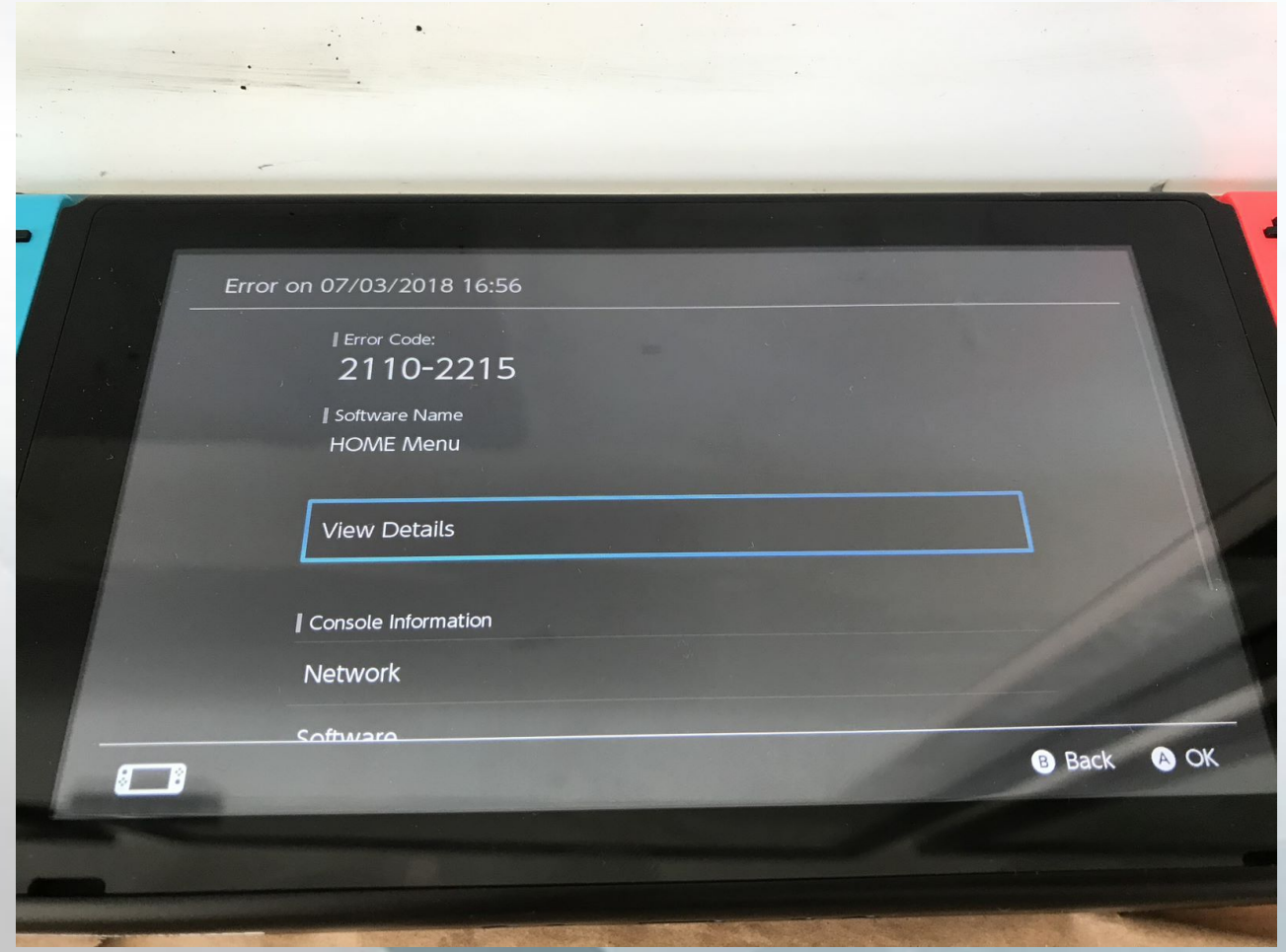


[dstl]

UNIVERSITY OF OXFORD

modux

Creation of Test Data

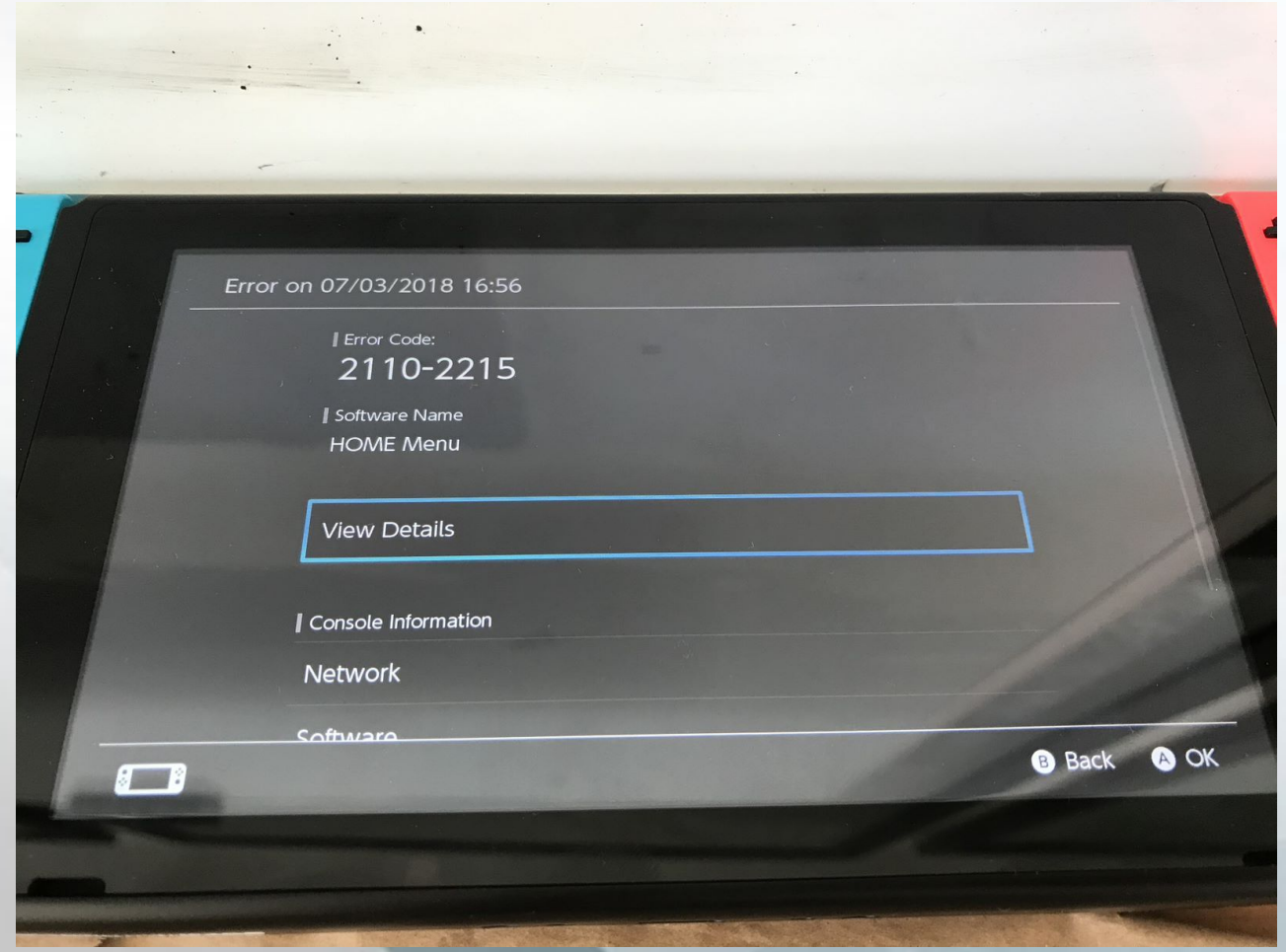


[dstl]

UNIVERSITY OF OXFORD

modux

Creation of Test Data



[dstl]

UNIVERSITY OF OXFORD

modux

Extraction of Data

```
PS E:\project-wario-demos\1a. demo-init-individual> move .\DumpNAND.ps1 .\DumpNANDPartition.ps1
PS E:\project-wario-demos\1a. demo-init-individual> .\DumpNANDPartition.ps1
Plug in Switch via usb-c in RCM mode to begin key dump
Once the keydump payload has completed, switch off the switch and restart into RCM mode
Win32 error 31 during post-smash read op
Key dump complete, please restart the Switch into RCM mode
TegraRcmSmash (64bit) 1.2.1-3 by rajkosto
Unknown key 'pwroffHoldTime' for BOOT section on line 12, skipping
Wanted device not connected yet, waiting...
Looking for devices matching the pattern *VID_0955&PID_7321*
Opened USB device path \\?\usb#vid_0955&pid_7321#6&11a6e85&0&2#{aa0dbd45-3117-f331-5c49-76bf65225042}
RCM Device with id 4085010C00000010C4072D6401101062 initialized successfully!
Uploading payload (mezzo size: 92, user size: 124720, total size: 190936, total padded size: 192512)...
Smashing the stack!
Smashed the stack with a 0x7000 byte SETUP request!
Switching to command mode due to READY.
Sending E:\project-wario-demos\1a. demo-init-individual\Tools\ums_emmc.scr.img (86 bytes) to address 0x80100000
Sending E:\project-wario-demos\1a. demo-init-individual\Tools\u-boot.elf (450879 bytes) to address 0x80110000
Booting AArch64 with PC 0x80110000...
BOOT command sent successfully! Continuing.
Win32 error 31 during post-smash read op
Mounting NAND. Please wait...
Starting NAND dump
```

[dstl]

UNIVERSITY OF OXFORD

modux

[dstl]

UNIVERSITY OF OXFORD

modux

Nintendo Switch Forensics

NAND File System

[dstl]

modux

NAND File System

- User Partitions
  - USER
    - FAT32 filesystem
    - Stores the data for all non-system applications
  - SYSTEM
    - FAT32 filesystem
    - Stores the data for all system applications
  - SAFE
    - FAT32 filesystem
    - Used for booting in SafeMode
  - PRODINFO
    - Used for system calibration.
  - PRODINFOF
    - Used for system calibration.

Partition Name	Details
USER	FAT32 Filesystem
SYSTEM	FAT32 Filesystem
SAFE	FAT32 Filesystem
PRODINFO	Used for System Calibration
PRODINFOF	Used for System Calibration

[dstl]

UNIVERSITY OF OXFORD

modux

NAND File System

- User Partitions
  - USER
    - FAT32 filesystem
    - Stores the data for all non-system applications
  - SYSTEM
    - FAT32 filesystem
    - Stores the data for all system applications
  - SAFE
    - FAT32 filesystem
    - Used for booting in SafeMode
  - PRODINFO
    - Used for system calibration.
  - PRODINFOF
    - Used for system calibration.

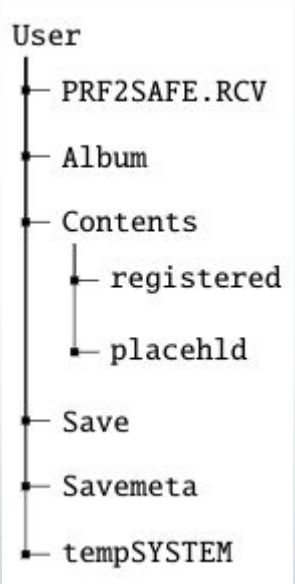
[dstl]

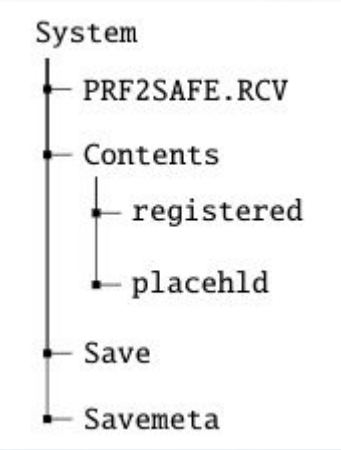
UNIVERSITY OF OXFORD

modux

NAND File System

- User Partitions
  - USER
    - FAT32 filesystem
    - Stores the data for all non-system applications
  - SYSTEM
    - FAT32 filesystem
    - Stores the data for all system applications



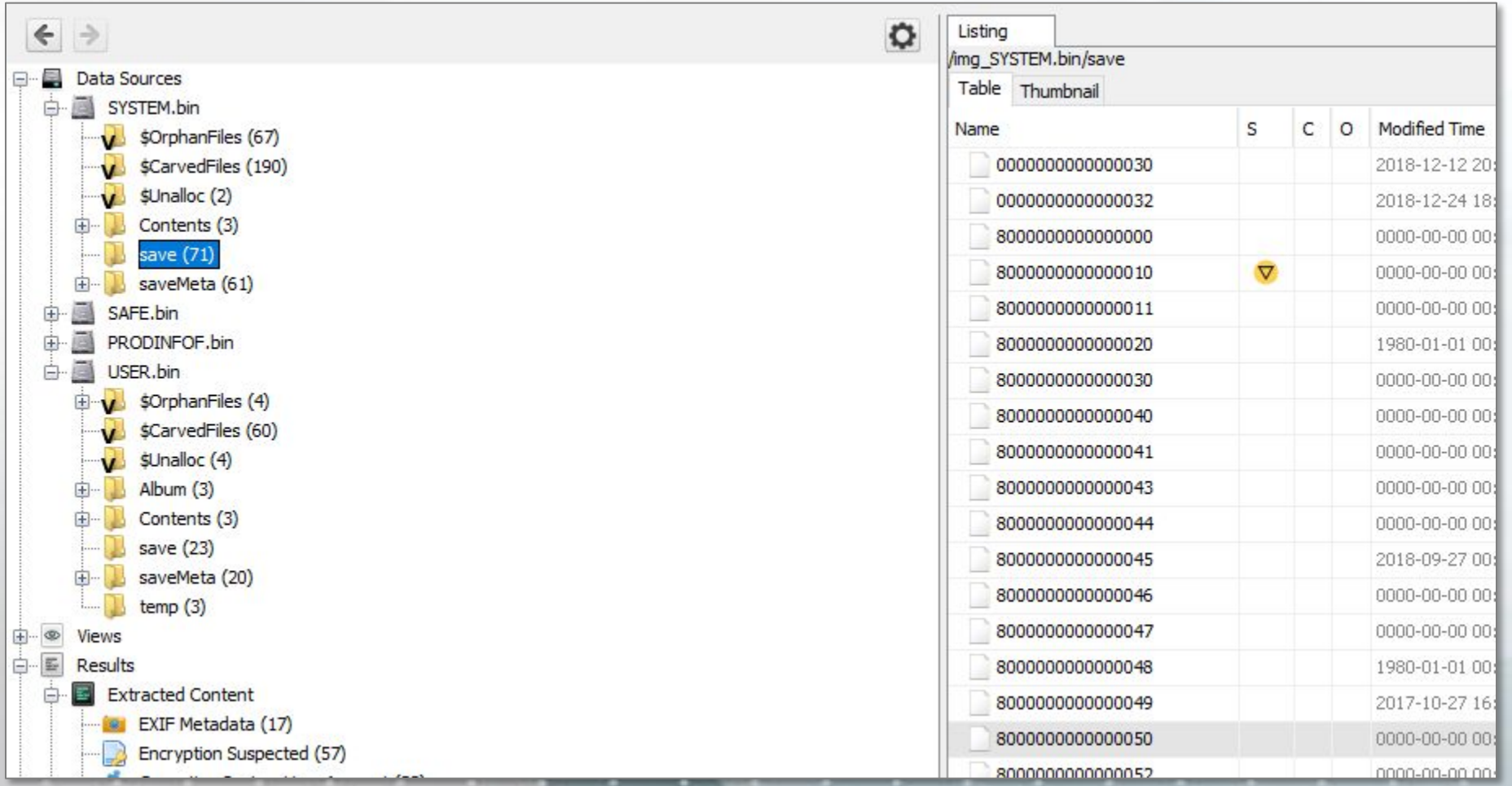


[dstl]

UNIVERSITY OF OXFORD

modux

NAND File System



[dstl]

UNIVERSITY OF OXFORD

modux

Nintendo Switch Forensics

Forensic Artefacts

[dstl]

modux

Artefact	Location	Available Data
Connected Displays	/SYSTEM.bin/save/80000000000000d1	Connected Displays
Error Logs	/SYSTEM.bin/save/80000000000000d1	Last 50 Error Codes
Game Saves	/USER.bin/save/	Save Time & Game Title
Gameplay Logs	/SYSTEM.bin/save/80000000000000a2	Access Time & Game Title
Multiplayer User History	/SYSTEM.bin/save/8000000000000001	300 users last played with
Power On/Off Logs	/SYSTEM.bin/save/80000000000000a1	Last Boot Time & Power State Changes
Screenshots & Videos	/SYSTEM.bin/	.JPG, .MP4 & .PNG with Timestamps
User Accounts	/SYSTEM.bin/save/8000000000000010	Birth Date, Email, Gender & Location
Wifi Networks	/SYSTEM.bin/save/8000000000000050	MAC Addresses, NAT, Passwords & SSIDs

[dstl]

UNIVERSITY OF OXFORD

modux

Artefacts – Device User Accounts

/img_SYSTEM.bin/save/8000000000000010

```
00077FE2  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
00078000  7B 22 67 65 6E 64 65 72 22 3A 22 6D 61 6C 65 22 2C 22 69 64 22 3A 22 64 66 61 66 39 31 36  {"gender":"male","id":"dfaf916
0007801E  31 35 64 33 37 34 61 66 63 22 2C 22 72 65 67 69 6F 6E 22 3A 22 22 2C 22 6C 6F 67 69 6E 49  15d374afc","region":"","loginI
0007803C  64 22 3A 22 22 2C 22 74 69 6D 65 7A 6F 6E 65 22 3A 22 45 75 72 6F 70 65 2F 4C 6F 6E 64 6F  d":"","timezone":"Europe/Londo
0007805A  6E 22 2C 22 65 6D 61 69 6C 22 3A 22 74 6F 6D 66 2B 77 61 6C 75 69 67 69 2D 73 77 69 74 63  n","email":"tomf+waluigi-switc
00078078  68 40 6D 6F 64 75 78 2E 63 6F 2E 75 6B 22 2C 22 61 6E 61 6C 79 74 69 63 73 46 6F 72 49 6E  h@modux.co.uk","analyticsForIn
00078096  74 65 72 6E 61 6C 41 6E 61 6C 79 73 69 73 50 65 72 6D 69 74 74 65 64 22 3A 74 72 75 65 2C  ternalAnalysisPermitted":true,
000780B4  22 61 6E 61 6C 79 74 69 63 73 46 6F 72 54 61 72 67 65 74 4D 61 72 6B 65 74 69 6E 67 50 65  "analyticsForTargetMarketingPe
000780D2  72 6D 69 74 74 65 64 22 3A 74 72 75 65 2C 22 6E 69 63 6B 6E 61 6D 65 22 3A 22 77 61 6C 75  rmitted":true,"nickname":"walu
000780F0  69 67 69 22 2C 22 73 63 72 65 65 6E 4E 61 6D 65 22 3A 22 74 6F E2 80 A2 E2 80 A2 E2 80 A2  igi","screenName":"toâ€¢â€¢â€¢
0007810E  40 6D E2 80 A2 E2 80 A2 E2 80 A2 E2 80 A2 22 2C 22 69 73 43 68 69 6C 64 22 3A 66 61 6C 73  @mâ€¢â€¢â€¢â€¢","isChild":fals
0007812C  65 2C 22 6C 61 6E 67 75 61 67 65 22 3A 22 65 6E 2D 47 42 22 2C 22 62 69 72 74 68 64 61 79  e,"language":"en-GB","birthday
0007814A  22 3A 22 32 30 30 30 2D 30 31 2D 30 31 22 2C 22 63 6F 75 6E 74 72 79 22 3A 22 47 42 22 2C  ":"2000-01-01","country":"GB",
00078168  22 69 73 4E 6E 4C 69 6E 6B 65 64 22 3A 66 61 6C 73 65 2C 22 69 73 54 77 69 74 74 65 72 4C  "isNnLinked":false,"isTwitterL
00078186  69 6E 6B 65 64 22 3A 66 61 6C 73 65 2C 22 69 73 46 61 63 65 62 6F 6F 6B 4C 69 6E 6B 65 64  inked":false,"isFacebookLinked
000781A4  22 3A 66 61 6C 73 65 2C 22 69 73 47 6F 6F 67 6C 65 4C 69 6E 6B 65 64 22 3A 66 61 6C 73 65  ":false,"isGoogleLinked":false
000781C2  7D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  }...............................
000781E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
```

[dstl]

UNIVERSITY OF OXFORD

modux

Artefacts – Device User Accounts


```
{
  "gender": "male",
  "id": "dfaf91615d374afc",
  "region": "",
  "loginId": "",
  "timezone": "Europe/London",
  "email": "----+----------@modux.co.uk",
  "analyticsForInternalAnalysisPermitted": true,
  "analyticsForTargetMarketingPermitted": true,
  "nickname": "waluigi",
  "screenName": "toâ€¢â€¢â€¢@mâ€¢â€¢â€¢â€¢",
  "isChild": false,
  "language": "en-GB",
  "birthday": "2000-01-01",
  "country": "GB",
  "isNnLinked": false,
  "isTwitterLinked": false,
  "isFacebookLinked": false,
  "isGoogleLinked": false
}
```

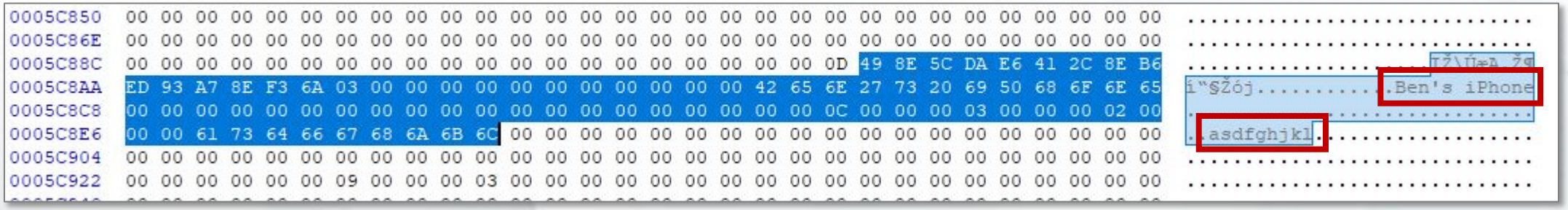

[dstl]

UNIVERSITY OF OXFORD

modux

Artefacts – Wi-Fi

/img_SYSTEM.bin/save/8000000000000050



[dstl]

UNIVERSITY OF OXFORD

modux

Artefacts – Connected Displays

/img_SYSTEM.bin/save/8000000000000050

```
00055A46  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
00055A64  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
00055A82  00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00 00 00 80 3F 00 00 00 3F 0C 00 00 00 00  ......................€?...?....
00055AA0  00 FF FF FF FF FF FF 00 09 D1 CE 78 45 54 00 00 03 19 01 03 80 35 1E 78 2E 6B 35 A4 55 55  .ÿÿÿÿÿÿ..ÑÎxET......€5.x.k5¤UU
00055ABE  9F 27 0C 50 54 A5 6B 80 D1 C0 81 C0 81 00 81 80 A9 C0 B3 00 01 01 01 01 02 3A 80 18 71 38  Ÿ'.PT¥k€ÑÀ.À...€©À³.....:€.q8
00055ADC  2D 40 58 2C 45 00 13 2B 21 00 00 1E 00 00 00 FF 00 54 31 46 30 31 39 35 34 53 4C 30 0A 20  -@X,E..+!.....ÿ.T1F01954SL0.
00055AFA  00 00 00 FD 00 32 4C 1E 53 11 00 0A 20 20 20 20 20 20 00 00 00 FC 00 42 65 6E 51 20 47 4C  ...ý.2L.S...      ...ü.BenQ GL
00055B18  32 34 36 30 0A 20 01 83 02 03 22 F1 4F 90 05 04 03 02 01 11 12 13 14 06 07 15 16 1F 23 09  2460. .ƒ.."ñO..............#.
00055B36  07 07 65 03 0C 00 10 00 83 01 00 00 02 3A 80 18 71 38 2D 40 58 2C 45 00 13 2B 21 00 00 1F  ..e.....ƒ....:€.q8-@X,E..+!...
00055B54  01 1D 80 18 71 1C 16 20 58 2C 25 00 13 2B 21 00 00 9F 01 1D 00 72 51 D0 1E 20 6E 28 55 00  ..€.q.. X,%..+!..Ÿ...rQÐ. n(U.
00055B72  13 2B 21 00 00 1E 8C 0A D0 8A 20 E0 2D 10 10 3E 96 00 13 2B 21 00 00 18 00 00 00 00 00 00  .+!...Œ.ÐŠ à-..>-..+!.........
00055B90  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 E7 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...............ç..............
00055BAE  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
```

[dstl]

UNIVERSITY OF OXFORD

modux

Artefacts – Connected Displays

Hex Dump 7 - Connected Display Model:

```
00059200 70 70 65 64 D2 00 00 45 17 A9 45 64 69 64 42 6C |pped...E..EdidBl|
00059210 6F 63 6B C4 80 00 FF FF FF FF FF FF 00 09 D1 CE |ock.............|
00059220 78 45 54 00 00 03 19 01 03 80 35 1E 78 2E 6B 35 |xET.......5.x.k5|
00059230 A4 55 55 9F 27 0C 50 54 A5 6B 80 D1 C0 81 C0 81 |.UU.'.PT.k......|
00059240 00 81 80 A9 C0 B3 00 01 01 01 01 02 3A 80 18 71 |............:..q|
00059250 38 2D 40 58 2C 45 00 13 2B 21 00 00 1E 00 00 00 |8-@X,E..+!......|
00059260 FF 00 54 31 46 30 31 39 35 34 53 4C 30 0A 20 00 |..T1F01954SL0. .|
00059270 00 00 FD 00 32 4C 1E 53 11 00 0A 20 20 20 20 20 |....2L.S...     |
00059280 20 00 00 00 FC 00 42 65 6E 51 20 47 4C 32 34 36 | .....BenQ GL246|
00059290 30 0A 20 01 83 B2 45 64 69 64 45 78 74 65 6E 73 |0. ...EdidExtens|
000592A0 69 6F 6E 42 6C 6F 63 6B C4 80 02 03 22 F1 4F 90 |ionBlock....".O.|
```

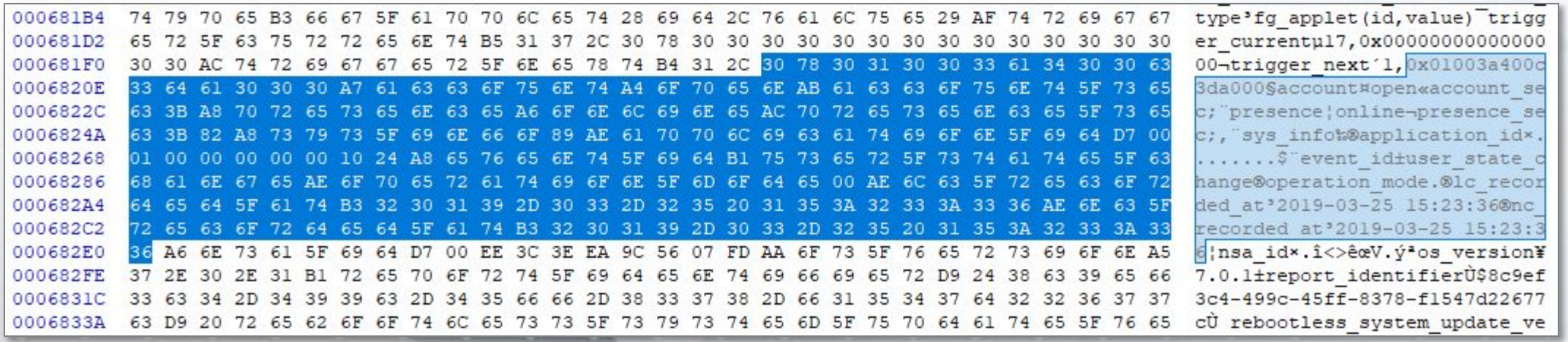
[dstl]

UNIVERSITY OF OXFORD

modux

Artefacts – Played games

/img_SYSTEM.bin/save/8000000000000a1



```
000681B4  74 79 70 65 B3 66 67 5F 61 70 70 6C 65 74 28 69 64 2C 76 61 6C 75 65 29 AF 74 72 69 67 67  type³fg_applet(id,value)¯trigg
000681D2  65 72 5F 63 75 72 72 65 6E 74 B5 31 37 2C 30 78 30 30 30 30 30 30 30 30 30 30 30 30 30 30  er_currentµ17,0x00000000000000
000681F0  30 30 AC 74 72 69 67 67 65 72 5F 6E 65 78 74 B4 31 2C 30 78 30 31 30 30 33 61 34 30 30 63  00¬trigger_next´1,0x01003a400c
0006820E  33 64 61 30 30 30 A7 61 63 63 6F 75 6E 74 A4 6F 70 65 6E AB 61 63 63 6F 75 6E 74 5F 73 65  3da000§account¤open«account_se
0006822C  63 3B A8 70 72 65 73 65 6E 63 65 A6 6F 6E 6C 69 6E 65 AC 70 72 65 73 65 6E 63 65 5F 73 65  c;¨presence¦online¬presence_se
0006824A  63 3B 82 A8 73 79 73 5F 69 6E 66 6F 89 AE 61 70 70 6C 69 63 61 74 69 6F 6E 5F 69 64 D7 00  c;‚¨sys_info‰®application_id×.
00068268  01 00 00 00 00 00 10 24 A8 65 76 65 6E 74 5F 69 64 B1 75 73 65 72 5F 73 74 61 74 65 5F 63  .......$¨event_id±user_state_c
00068286  68 61 6E 67 65 AE 6F 70 65 72 61 74 69 6F 6E 5F 6D 6F 64 65 00 AE 6C 63 5F 72 65 63 6F 72  hange®operation_mode.®lc_recor
000682A4  64 65 64 5F 61 74 B3 32 30 31 39 2D 30 33 2D 32 35 20 31 35 3A 32 33 3A 33 36 AE 6E 63 5F  ded_at³2019-03-25 15:23:36®nc_
000682C2  72 65 63 6F 72 64 65 64 5F 61 74 B3 32 30 31 39 2D 30 33 2D 32 35 20 31 35 3A 32 33 3A 33  recorded_at³2019-03-25 15:23:3
000682E0  36 A6 6E 73 61 5F 69 64 D7 00 EE 3C 3E EA 9C 56 07 FD AA 6F 73 5F 76 65 72 73 69 6F 6E A5  6¦nsa_id×.î<>êœV.ý²os_version¥
000682FE  37 2E 30 2E 31 B1 72 65 70 6F 72 74 5F 69 64 65 6E 74 69 66 69 65 72 D9 24 38 63 39 65 66  7.0.1±report_identifierÙ$8c9ef
0006831C  33 63 34 2D 34 39 39 63 2D 34 35 66 66 2D 38 33 37 38 2D 66 31 35 34 37 64 32 32 36 37 37  3c4-499c-45ff-8378-f1547d22677
0006833A  63 D9 20 72 65 62 6F 6F 74 6C 65 73 73 5F 73 79 73 74 65 6D 5F 75 70 64 61 74 65 5F 76 65  cÙ rebootless_system_update_ve
```

[dstl]

UNIVERSITY OF OXFORD

modux

Artefacts – Youtube Searches

```
0005038E  34 34 39 7D 12 9E 01 0A 33 79 74 2E 6C 65 61 6E 62 61 63 6B 2E 64 65 66 61 75 6C 74 2E 73  449}.ž..3yt.leanback.default.s
000503AC  65 61 72 63 68 2D 68 69 73 74 6F 72 79 3A 3A 72 65 63 65 6E 74 2D 73 65 61 72 63 68 65 73  earch-history::recent-searches
000503CA  12 67 7B 22 64 61 74 61 22 3A 5B 5B 22 62 65 73 74 20 73 70 6F 6E 67 65 62 6F 62 20 73 6F  .g{"data":[["best spongebob so
000503E8  6E 67 73 22 2C 32 2C 31 35 35 31 39 37 38 37 35 38 30 36 31 5D 5D 2C 22 65 78 70 69 72 61  ngs",2,1551978758061]],"expira
00050406  74 69 6F 6E 22 3A 31 35 38 33 30 38 32 37 35 38 30 36 32 2C 22 63 72 65 61 74 69 6F 6E 22  tion":1583082758062,"creation"
00050424  3A 31 35 35 31 39 37 38 37 35 38 30 36 32 7D 12 74 0A 32 79 74 2E 6C 65 61 6E 62 61 63 6B  :1551978758062}.t.2yt.leanback
```

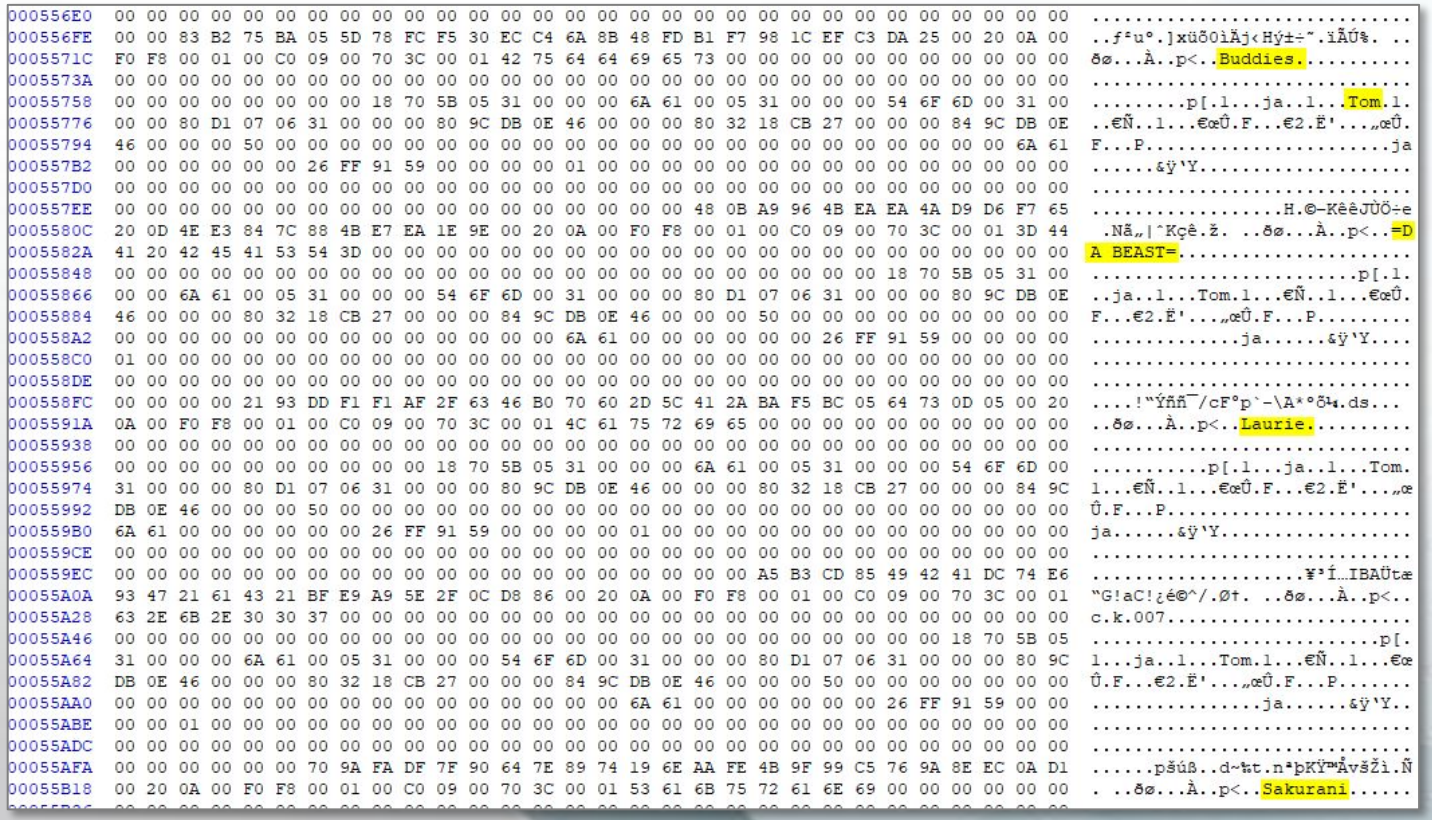
[dstl]

UNIVERSITY OF OXFORD

modux

Artefacts – Players played with

/img_SYSTEM.bin/save/8000000000000001



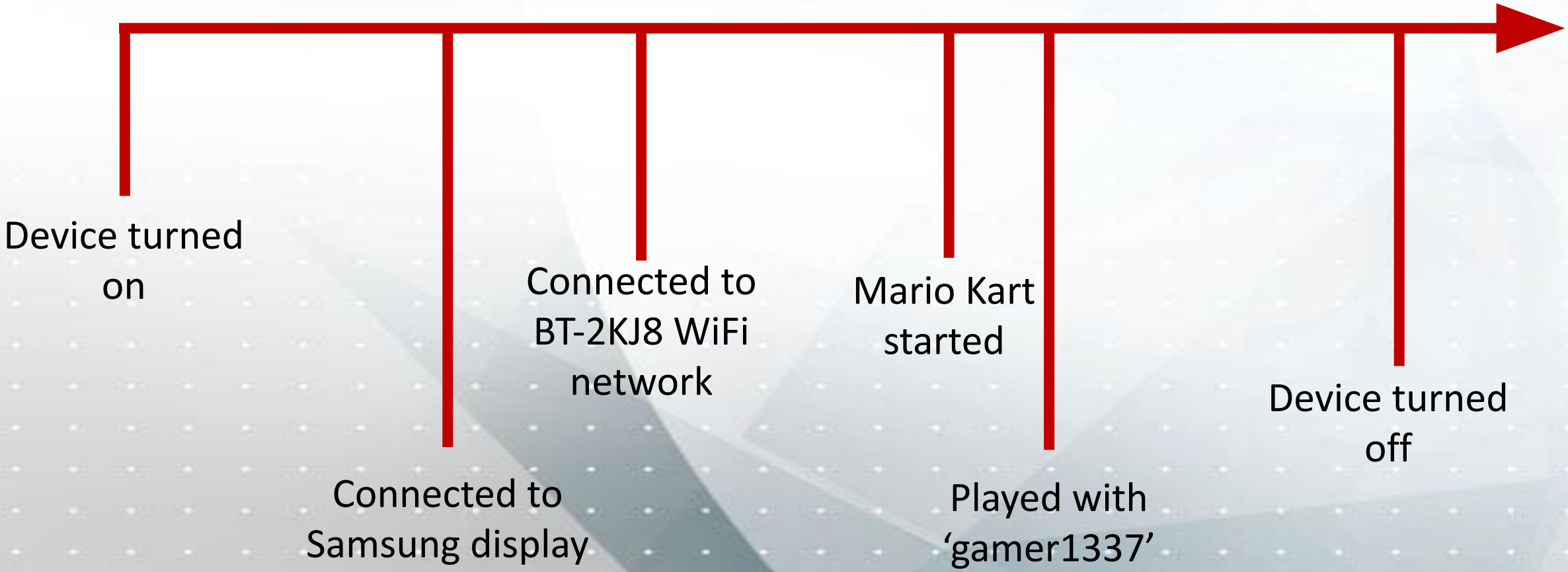
```
000556E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
000556FE  00 00 83 B2 75 BA 05 5D 78 FC F5 30 EC C4 6A 8B 48 FD B1 F7 98 1C EF C3 DA 25 00 20 0A 00  ..ƒ²u°.]xüõ0ìÄj‹Hý±÷˜.ïÃÚ%. ..
0005571C  F0 F8 00 01 00 C0 09 00 70 3C 00 01 42 75 64 64 69 65 73 00 00 00 00 00 00 00 00 00 00 00  ðø...À..p<..Buddies.............
0005573A  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
00055758  00 00 00 00 00 00 00 00 18 70 5B 05 31 00 00 00 6A 61 00 05 31 00 00 00 54 6F 6D 00 31 00  .........p[.1...ja..1...Tom.1.
00055776  00 00 80 D1 07 06 31 00 00 00 80 9C DB 0E 46 00 00 00 80 32 18 CB 27 00 00 00 84 9C DB 0E  ..€Ñ..1...€œÛ.F...€2.Ë'...„œÛ.
00055794  46 00 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6A 61  F...P.......................ja
000557B2  00 00 00 00 00 00 26 FF 91 59 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ......&ÿ'Y.....................
000557D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
000557EE  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 0B A9 96 4B EA EA 4A D9 D6 F7 65  ..................H.©–KêêJÙÖ÷e
0005580C  20 0D 4E E3 84 7C 88 4B E7 EA 1E 9E 00 20 0A 00 F0 F8 00 01 00 C0 09 00 70 3C 00 01 3D 44  .Nã„|ˆKçê.ž. ..ðø...À..p<..=D
0005582A  41 20 42 45 41 53 54 3D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  A BEAST=........................
00055848  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 70 5B 05 31 00  ..........................p[.1.
00055866  00 00 6A 61 00 05 31 00 00 00 54 6F 6D 00 31 00 00 00 80 D1 07 06 31 00 00 00 80 9C DB 0E  ..ja..1...Tom.1...€Ñ..1...€œÛ.
00055884  46 00 00 00 80 32 18 CB 27 00 00 00 84 9C DB 0E 46 00 00 00 50 00 00 00 00 00 00 00 00 00  F...€2.Ë'...„œÛ.F...P.........
000558A2  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6A 61 00 00 00 00 00 00 26 FF 91 59 00 00 00 00  ..............ja......&ÿ'Y....
000558C0  01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
000558DE  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
000558FC  00 00 00 00 21 93 DD F1 F1 AF 2F 63 46 B0 70 60 2D 5C 41 2A BA F5 BC 05 64 73 0D 05 00 20  ....!"Ýññ¯/cF°p`-\A*°õ¼.ds...
0005591A  0A 00 F0 F8 00 01 00 C0 09 00 70 3C 00 01 4C 61 75 72 69 65 00 00 00 00 00 00 00 00 00 00  ..ðø...À..p<..Laurie............
00055938  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
00055956  00 00 00 00 00 00 00 00 00 00 18 70 5B 05 31 00 00 00 6A 61 00 05 31 00 00 00 54 6F 6D 00  ...........p[.1...ja..1...Tom.
00055974  31 00 00 00 80 D1 07 06 31 00 00 00 80 9C DB 0E 46 00 00 00 80 32 18 CB 27 00 00 00 84 9C  1...€Ñ..1...€œÛ.F...€2.Ë'...„œ
00055992  DB 0E 46 00 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  Û.F...P.........................
000559B0  6A 61 00 00 00 00 00 00 26 FF 91 59 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00  ja......&ÿ'Y...................
000559CE  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
000559EC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 A5 B3 CD 85 49 42 41 DC 74 E6  ....................¥³Í…IBAÜtæ
00055A0A  93 47 21 61 43 21 BF E9 A9 5E 2F 0C D8 86 00 20 0A 00 F0 F8 00 01 00 C0 09 00 70 3C 00 01  "G!aC!¿é©^/.Ø†. ..ðø...À..p<..
00055A28  63 2E 6B 2E 30 30 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  c.k.007.........................
00055A46  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 70 5B 05  ..............................p[.
00055A64  31 00 00 00 6A 61 00 05 31 00 00 00 54 6F 6D 00 31 00 00 00 80 D1 07 06 31 00 00 00 80 9C  1...ja..1...Tom.1...€Ñ..1...€œ
00055A82  DB 0E 46 00 00 00 80 32 18 CB 27 00 00 00 84 9C DB 0E 46 00 00 00 50 00 00 00 00 00 00 00  Û.F...€2.Ë'...„œÛ.F...P.......
00055AA0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6A 61 00 00 00 00 00 00 26 FF 91 59  ..................ja......&ÿ'Y
00055ABE  00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
00055ADC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
00055AFA  00 00 00 00 00 00 70 9A FA DF 7F 90 64 7E 89 74 19 6E AA FE 4B 9F 99 C5 76 9A 8E EC 0A D1  ......pšúß..d~‰t.nªþKŸ™ÅvšŽì.Ñ
00055B18  00 20 0A 00 F0 F8 00 01 00 C0 09 00 70 3C 00 01 53 61 6B 75 72 61 6E 69 00 00 00 00 00 00  . ..ðø...À..p<..Sakurani......
```

[dstl]

UNIVERSITY OF OXFORD

modux

Device Timeline

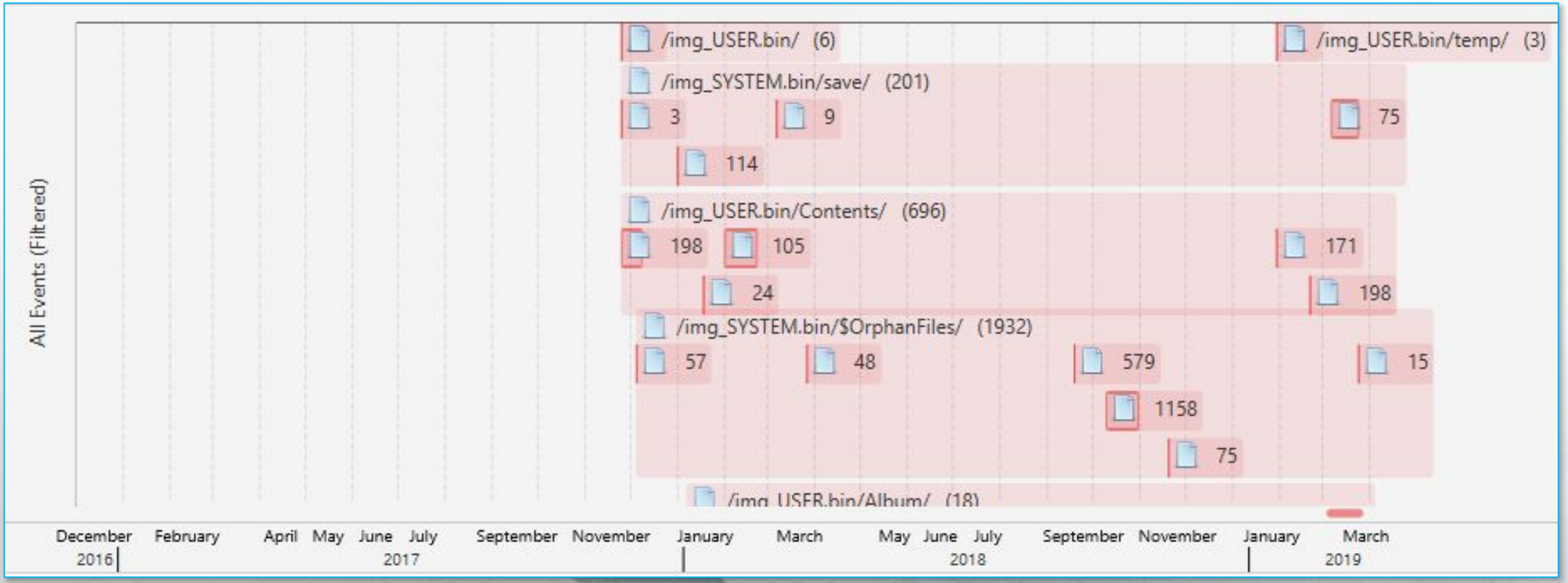


[dstl]

UNIVERSITY OF OXFORD

modux

Device Timeline



[dstl]

UNIVERSITY OF OXFORD

modux

Nintendo Switch Forensics

Autopsy Modules

[dstl]

modux

Autopsy Modules - Open Source

Nintendo-Switch-Forensics

Autopsy folder contains the following Autopsy ingest modules:

Module	Purpose
ingest_connected_displays	all recently connected displays
ingest_game_history	recent game history
ingest_crash_dumps	last 50 crash dumps
ingest_device_accounts	all user accounts saved to device
ingest_gamesaves	all saved games
ingest_last_boot	last boot time of device
ingest_mp_user_history	last 300 users played with and game played
ingest_power_states	device power history
ingest_screenshots	all saved recordings and screenshots
ingest_wifi	details of all WiFi networks recently connected to

memory-dump-utils folder contains utilities to aid in performing Switch memory dumps

[dstl]

UNIVERSITY OF OXFORD

modux

Autopsy Modules - Ingest Modules

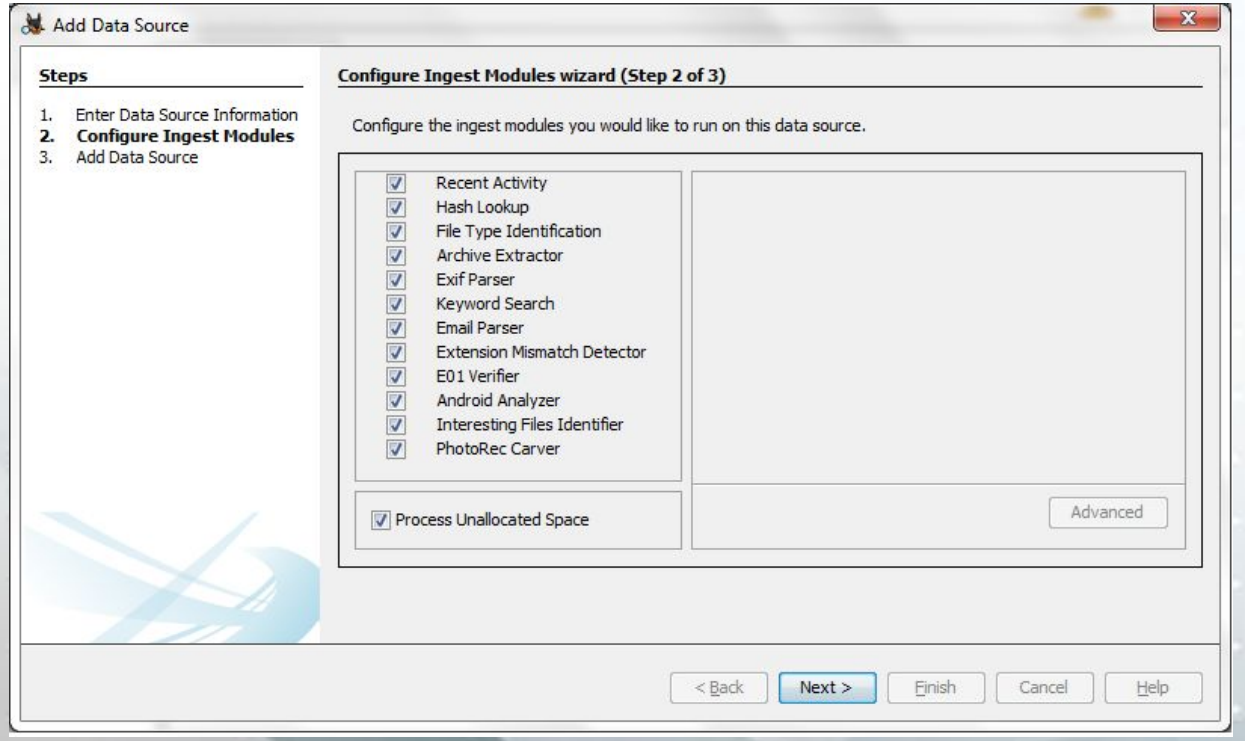
- Ingest Module Types
  - **Ingest Modules:** Run when new data sources are ingested
  - **Report Module:** Modules run after user has reviewed results and tagged files.

[dstl]

UNIVERSITY OF OXFORD

modux

Autopsy Modules - Ingest Modules

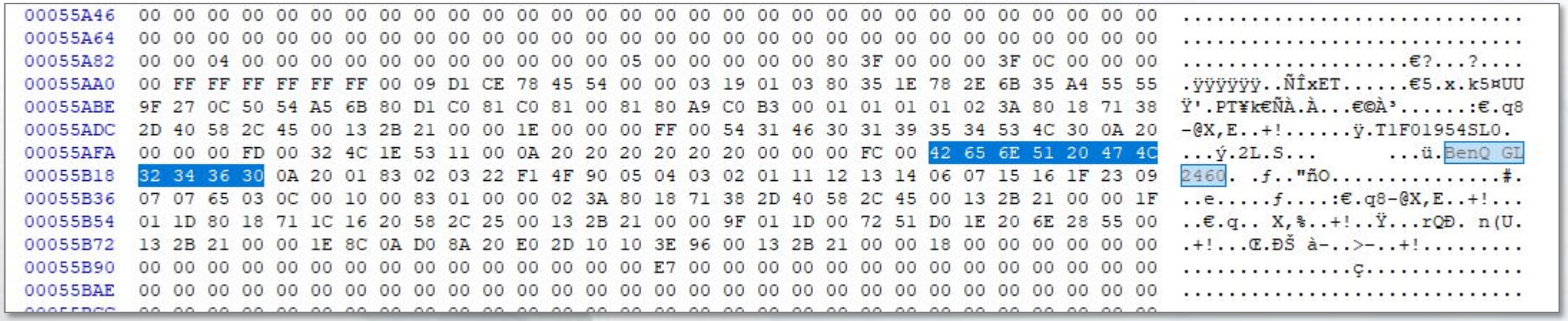


[dstl]

UNIVERSITY OF OXFORD

modux

Autopsy Modules - Connected TV's



```
00055A46  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..............................
00055A64  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..............................
00055A82  00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00 00 00 80 3F 00 00 00 3F 0C 00 00 00  ..................€?...?....
00055AA0  00 FF FF FF FF FF FF 00 09 D1 CE 78 45 54 00 00 03 19 01 03 80 35 1E 78 2E 6B 35 A4 55 55  .ÿÿÿÿÿÿ..ÑÎxET.....€5.x.k5¤UU
00055ABE  9F 27 0C 50 54 A5 6B 80 D1 C0 81 C0 81 00 81 80 A9 C0 B3 00 01 01 01 01 02 3A 80 18 71 38  Ÿ'.PT¥k€ÑÀ.À...€©À³.....:€.q8
00055ADC  2D 40 58 2C 45 00 13 2B 21 00 00 1E 00 00 00 FF 00 54 31 46 30 31 39 35 34 53 4C 30 0A 20  -@X,E..+!.....ÿ.T1F01954SL0.
00055AFA  00 00 00 FD 00 32 4C 1E 53 11 00 0A 20 20 20 20 20 20 00 00 00 FC 00 42 65 6E 51 20 47 4C  ...ý.2L.S...      ...ü.BenQ GL
00055B18  32 34 36 30 0A 20 01 83 02 03 22 F1 4F 90 05 04 03 02 01 11 12 13 14 06 07 15 16 1F 23 09  2460. .ƒ.."ñO..............#.
00055B36  07 07 65 03 0C 00 10 00 83 01 00 00 02 3A 80 18 71 38 2D 40 58 2C 45 00 13 2B 21 00 00 1F  ..e.....ƒ.....:€.q8-@X,E..+!...
00055B54  01 1D 80 18 71 1C 16 20 58 2C 25 00 13 2B 21 00 00 9F 01 1D 00 72 51 D0 1E 20 6E 28 55 00  ..€.q.. X,%..+!..Ÿ...rQÐ. n(U.
00055B72  13 2B 21 00 00 1E 8C 0A D0 8A 20 E0 2D 10 10 3E 96 00 13 2B 21 00 00 18 00 00 00 00 00 00  .+!...Œ.ĐŠ à-..>-..+!.........
00055B90  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 E7 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...............ç...............
00055BAE  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..............................
```

[dstl]

UNIVERSITY OF OXFORD

modux

Autopsy Modules - Development Process

```
if file.getName() == "80000000000000d1":
    artifactList = file.getArtifacts(ARTID_NS_TV)

    self.log(Level.INFO, "Found the file" + file.getName())
    self.filesFound += 1

    inputStream = ReadContentInputStream(file)
    buffer = jarray.zeros(2048, "b")
    totLen = 0
    lengthofbuffer = inputStream.read(buffer)
    while lengthofbuffer != -1:
        totLen = totLen + lengthofbuffer
        lengthofbuffer = inputStream.read(buffer)
        currentBuffer = buffer.tostring()
        names = names + re.findall("EdidBlock.*?\\\\xfc\\\\x00(.*?)\\\\n.*?EdidExtensionBlock", repr(currentBuffer))
```

[dstl]

UNIVERSITY OF OXFORD

modux

Discussion - Chain of Custody

Using a software exploit to image RAM on an embedded system

J.R. Rabaiotti, C.J. Hargreaves*

Centre for Forensic Computing and Security, Cranfield University, Shrivenham, UK

[dstl]

UNIVERSITY OF OXFORD

modux

Discussion - Ethics and Legality

U.S. Attorneys » Western District of Washington » News

Department of Justice

U.S. Attorney's Office

Western District of Washington

SHARE

FOR IMMEDIATE RELEASE — Friday, October 2, 2020

Two members of notorious videogame piracy group "Team Xecuter" in custody

Arrested on Indictment from Western District of Washington

Seattle — Two leaders of one of the world's most notorious videogame piracy groups, Team Xecuter, have been arrested and are in custody facing charges filed in U.S. District Court in Seattle.

[dstl]

UNIVERSITY OF OXFORD

modux

Discussion - Limitations

Name	Compatible firmware versions	Author(s)	Link	Status
Jamais vu	1.0.0	ReSwitched Team (SciresM, and Motezazer)	Thread, reddit	Fixed
PegaSwitch	1.0.0 - 3.0.0	ReSwitched Team (SciresM, and more)	website, Sources	Fixed
Nereba	1.0.0 - 3.0.0	ReSwitched Team (Stuckpixel)	Unofficial Thread, Sources	Fixed
Déjà Vu / Caffeine	1.0.0 - 4.1.0, partially up to 7.0.1	SciresM	Unofficial Thread, Unofficial Thread, github for 3.0.0, unofficial thread caffeine for 4.1.0 released	Fixed
Fusée Gelée	All (non iPatched consoles only)	Independently discovered by ReSwitched Team (Kate Temkin), fail0verflow (shuffle2).	Unofficial Thread	Fixed, june2018

[dstl]

UNIVERSITY OF OXFORD

modux

Future Work

[dstl]

UNIVERSITY OF OXFORD

modux

Questions?

https://modux.co.uk