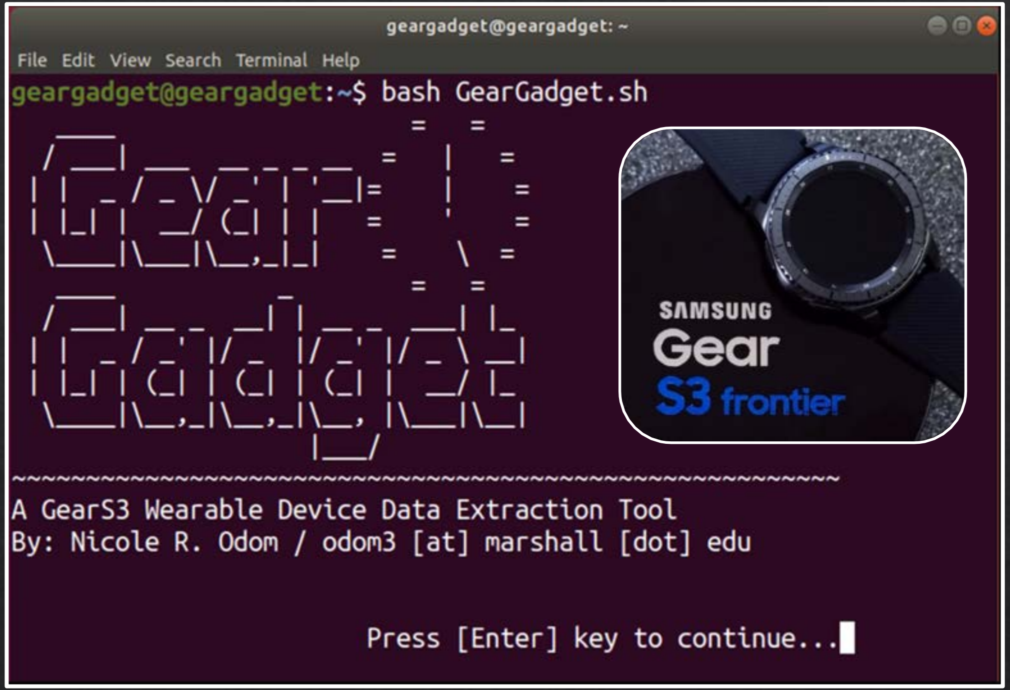
Go-Go Gadget Smartwatch:

Open Source Forensic Tools & Methodologies for Wearable Devices



```
geargadget@geargadget:~$ bash GearGadget.sh
                                  =    =
  ____                       =    |     =
 / ___| ___  __ _ _ __  =    |     =
| |  _ / _ \/ _` | '__|=     |      =
| |_| |  __/ (_| | |   =      \    =
 \____|\___|\__,_|_|   =       =
  ____           _            _
 / ___| __ _  __| | __ _  ___| |_
| |  _ / _` |/ _` |/ _` |/ _ \ __|
| |_| | (_| | (_| | (_| |  __/ |_
 \____|\__,_|\__,_|\__, |\___|\__|
                   |___/
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
A GearS3 Wearable Device Data Extraction Tool
By: Nicole R. Odom / odom3 [at] marshall [dot] edu


                        Press [Enter] key to continue...
```

Research Aims

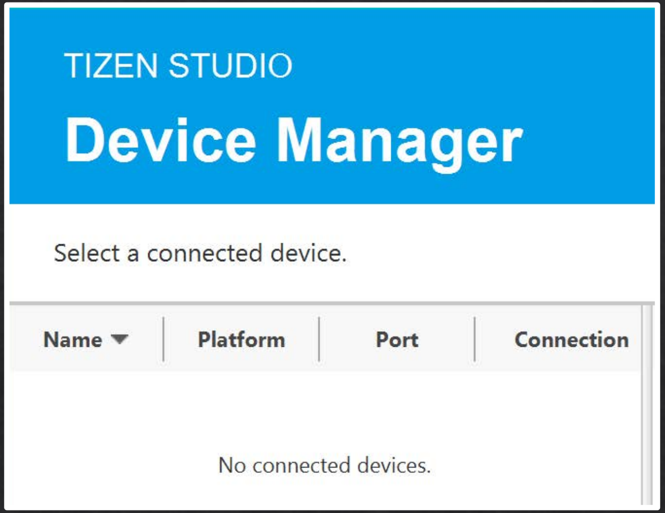
- Provide an enhanced understanding of:
  - Interaction between wearables and phones
  - Probative evidence wearables contain
  - Location of user data & artifacts storage
    - Standalone & Connected modes
  - Process to acquire data directly or indirectly

Connectivity

- ⟐ Connected Mode
  - Bluetooth & Wi-Fi
  - Pulls data from phone

- ⟐ Standalone Mode
  - eSIM
  - Pulls data from network

Connecting to PC



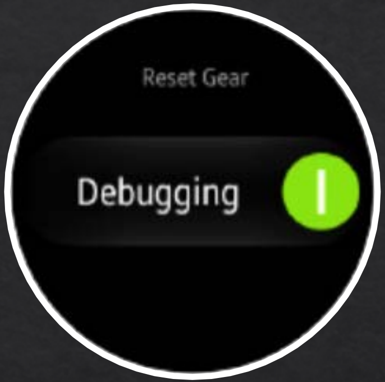
TIZEN STUDIO

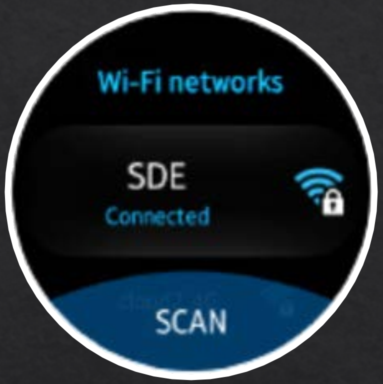
Device Manager

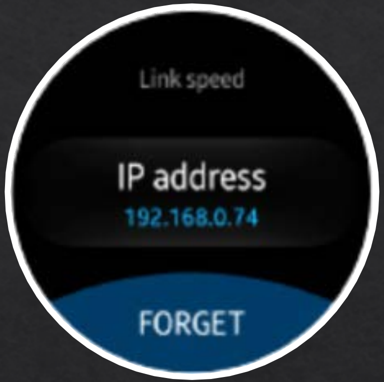
Select a connected device.

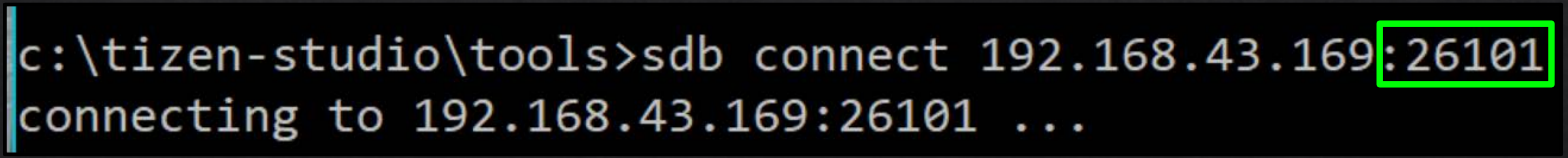
Name ▾	Platform	Port	Connection

No connected devices.

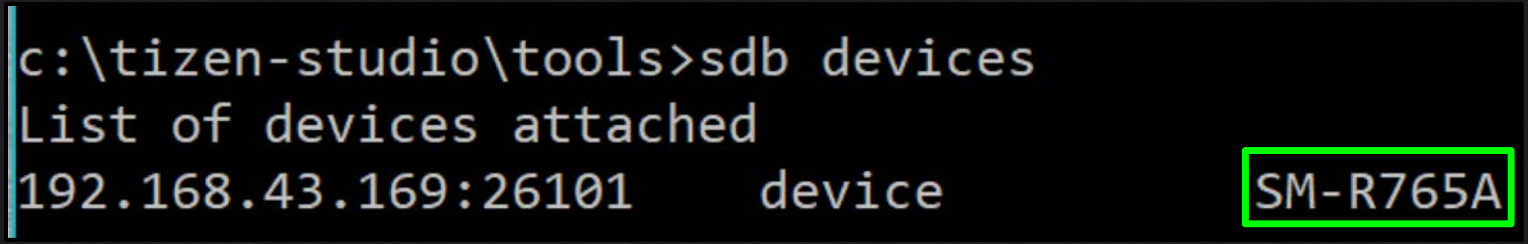




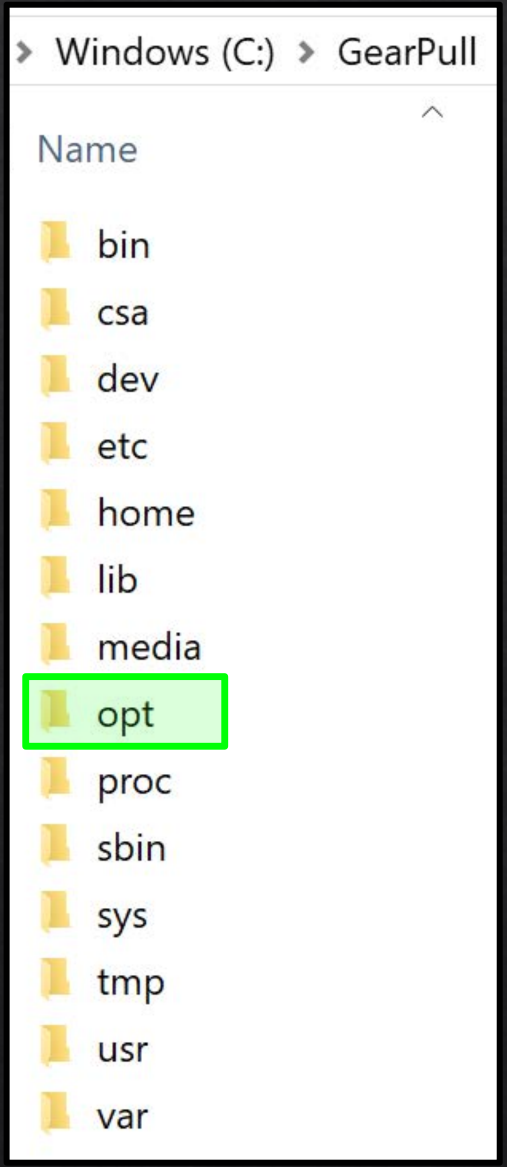




```
c:\tizen-studio\tools>sdb connect 192.168.43.169:26101
connecting to 192.168.43.169:26101 ...
```



```
c:\tizen-studio\tools>sdb devices
List of devices attached
192.168.43.169:26101    device          SM-R765A
```



Windows (C:) > GearPull

Name

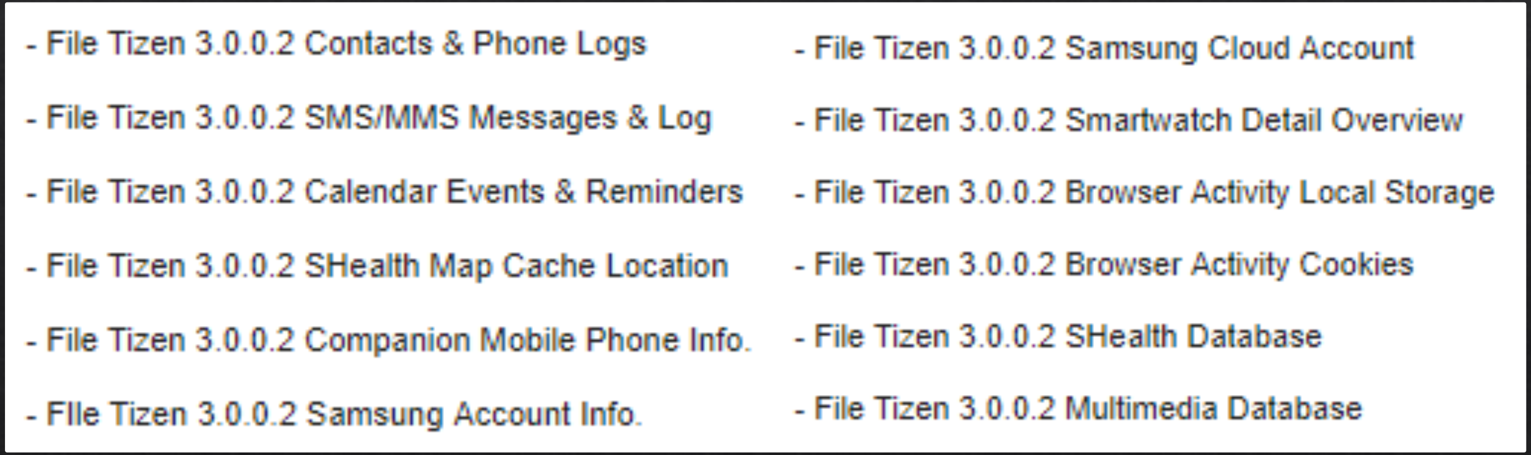
- bin
- csa
- dev
- etc
- home
- lib
- media
- opt
- proc
- sbin
- sys
- tmp
- usr
- var

Results

- Acquisition is equal, if not better than companion device
    - Opt directory
        - Contains duplicates of most, if not all, user data files
- User Data Exclusions
    - Connected
        - Some data local to phone: draft emails
        - SMS, MMS, or Browser Activity when in this state
    - Standalone
        - Deleted messages
        - Browser Activity excludes typed queries

Contributions

- Artifact Genome Project (AGP)
  - Started by University of New Haven
  - All identified novel artifacts submitted for referenece



- File Tizen 3.0.0.2 Contacts & Phone Logs
- File Tizen 3.0.0.2 SMS/MMS Messages & Log
- File Tizen 3.0.0.2 Calendar Events & Reminders
- File Tizen 3.0.0.2 SHealth Map Cache Location
- File Tizen 3.0.0.2 Companion Mobile Phone Info.
- FIle Tizen 3.0.0.2 Samsung Account Info.
- File Tizen 3.0.0.2 Samsung Cloud Account
- File Tizen 3.0.0.2 Smartwatch Detail Overview
- File Tizen 3.0.0.2 Browser Activity Local Storage
- File Tizen 3.0.0.2 Browser Activity Cookies
- File Tizen 3.0.0.2 SHealth Database
- File Tizen 3.0.0.2 Multimedia Database

- Accessible at: https://agp.newhaven.edu/

Contributions

- Journal of Forensic Sciences (JFS) publication
  - https://doi.org/10.1111/1556-4029.14109

JOURNAL OF FORENSIC SCIENCES

J Forensic Sci, 2019
doi: 10.1111/1556-4029.14109
Available online at: onlinelibrary.wiley.com

PAPER

DIGITAL & MULTIMEDIA SCIENCES

Nicole R. Odom,[1,2] *M.S.F.S. Jesse M. Lindmar,*[2] *B.S.; John Hirt,*[2] *B.S.; and Josh Brunty*,[1] *M.S.*

Forensic Inspection of Sensitive User Data and Artifacts from Smartwatch Wearable Devices*,†

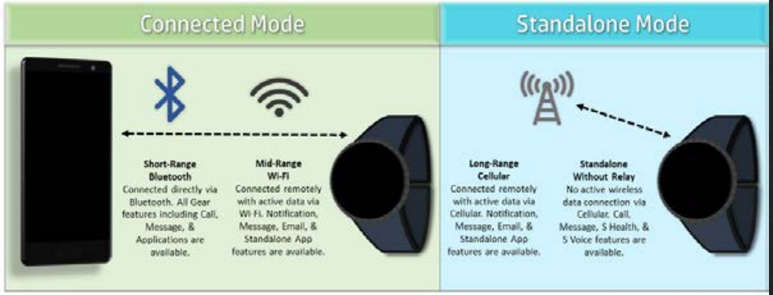
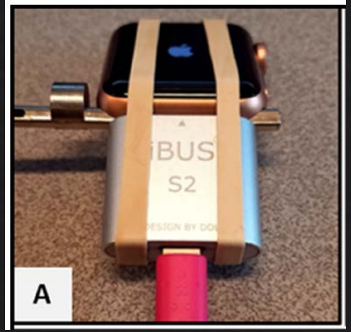
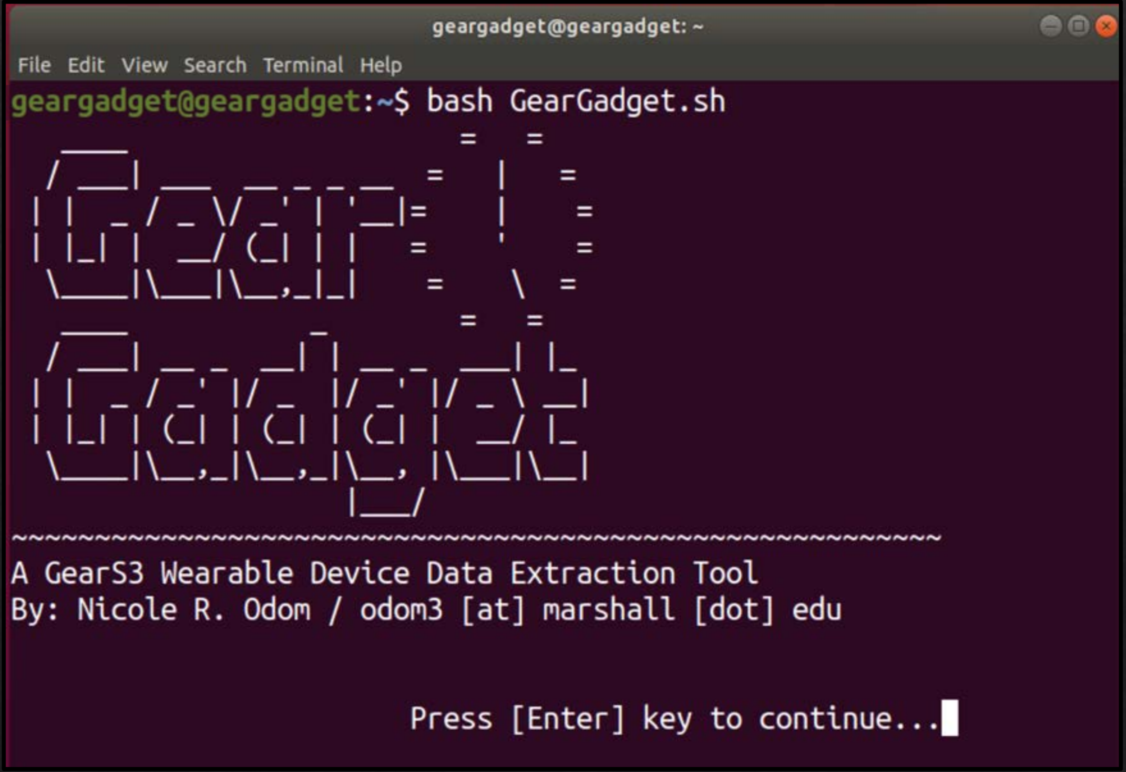

Connected Mode
Standalone Mode
Short-Range Bluetooth
Connected directly via Bluetooth. All Gear features including Call, Message, & Applications are available.
Mid-Range Wi-Fi
Connected remotely with active data via Wi-Fi. Notification, Message, Email, & Standalone App features are available.
Long-Range Cellular
Connected remotely with active data via Cellular. Notification, Message, Email, & Standalone App features are available.
Standalone Without Relay
No active wireless data connection via Cellular. Call, Message, S Health, & S Voice features are available.

FIG. 1—*Modes of operation & connectivity of the Samsung™ Gear S3 Frontier.*



GearGadget Demo

https://www.marshall.edu/cyber/geargadget/



```
geargadget@geargadget:~$ bash GearGadget.sh
   ____                    =   =
  / ___| ___  __ _ _ __  =   |   =
 | |  _ / _ \/ _` | '__|=    |    =
 | |_| |  __/ (_| | |   =    '    =
  \____|\___|\__,_|_|    =    \  =
   ____           _        =   = _
  / ___| __ _  __| | __ _  ___| |_
 | |  _ / _` |/ _` |/ _` |/ _ \ __|
 | |_| | (_| | (_| | (_| |  __/ |_
  \____|\__,_|\__,_|\__, |\___|\__|
                    |___/
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
A GearS3 Wearable Device Data Extraction Tool
By: Nicole R. Odom / odom3 [at] marshall [dot] edu


                        Press [Enter] key to continue...
```

LOG_02-05-19_Device1.txt

MD5_02-05-19_Device1.txt

Go-Go Gadget Smartwatch:

Open Source Forensic Tools & Methodologies for Wearable Devices

Contact Info

Nicole R. Odom, MSFS | ACE, CCO
Forensic Scientist
Digital & Multimedia Evidence Section
Virginia Department of Forensic Science
Email: *Nicole.Odom@dfs.virginia.gov*

Josh Brunty, MS | SCERS, CCME, CHFI, CFVT, ACE, MCFE
Associate Professor
Digital Forensics & Information Assurance
Marshall University Forensic Science Center
Email: *Josh.Brunty@marshall.edu*