
University of Colorado Boulder

Final Project

Joe McManus
Interdisciplinary Telecommunications Program
University of Colorado

Final Project

- **Due 5/2**
- **Presentations 5/2 and 5/4**
- **Groups of 2**

IoT

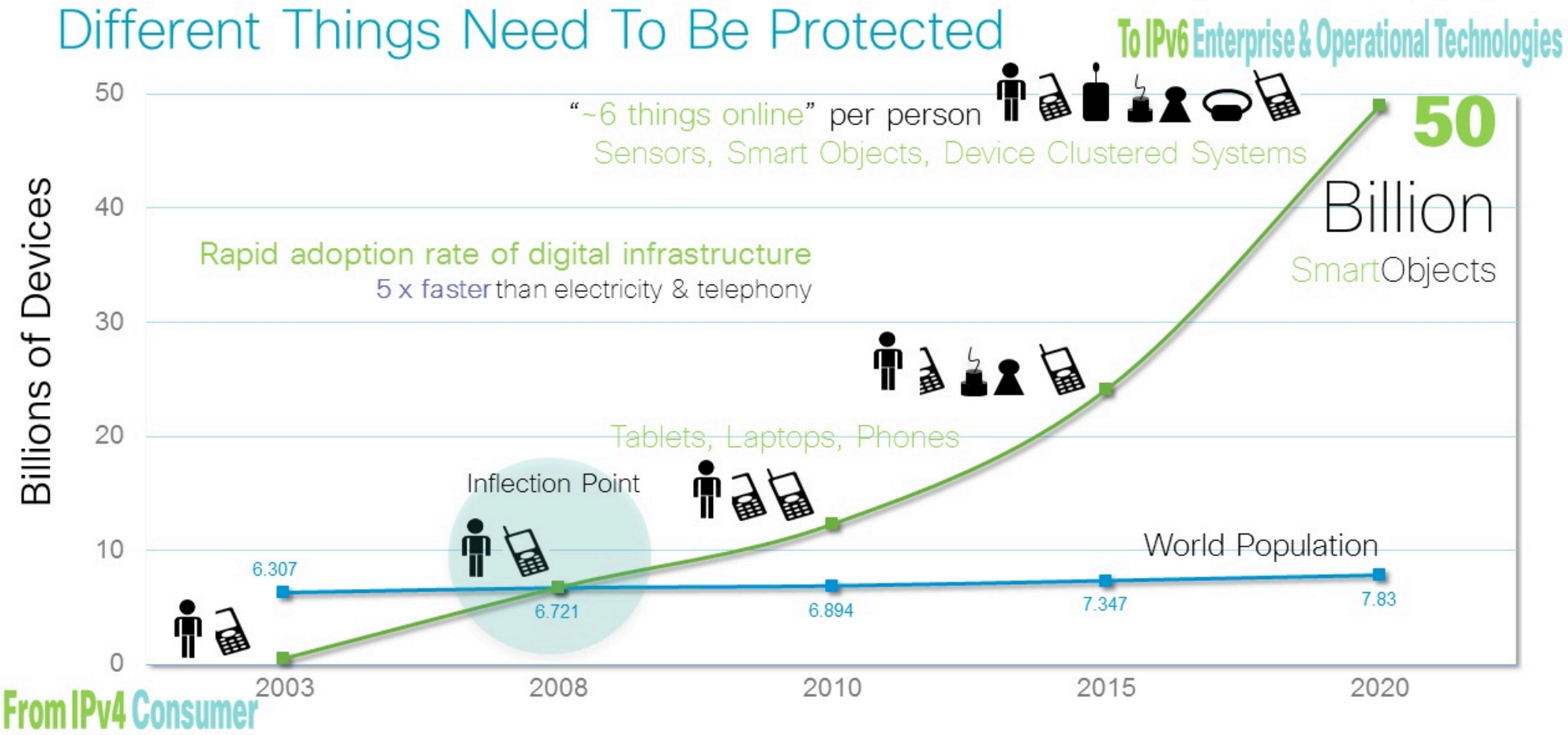
- **The internet of things (IoT) is a new name for an already existing technology like SCADA.**

- **How do you perform forensics analysis on these devices?**

IoT

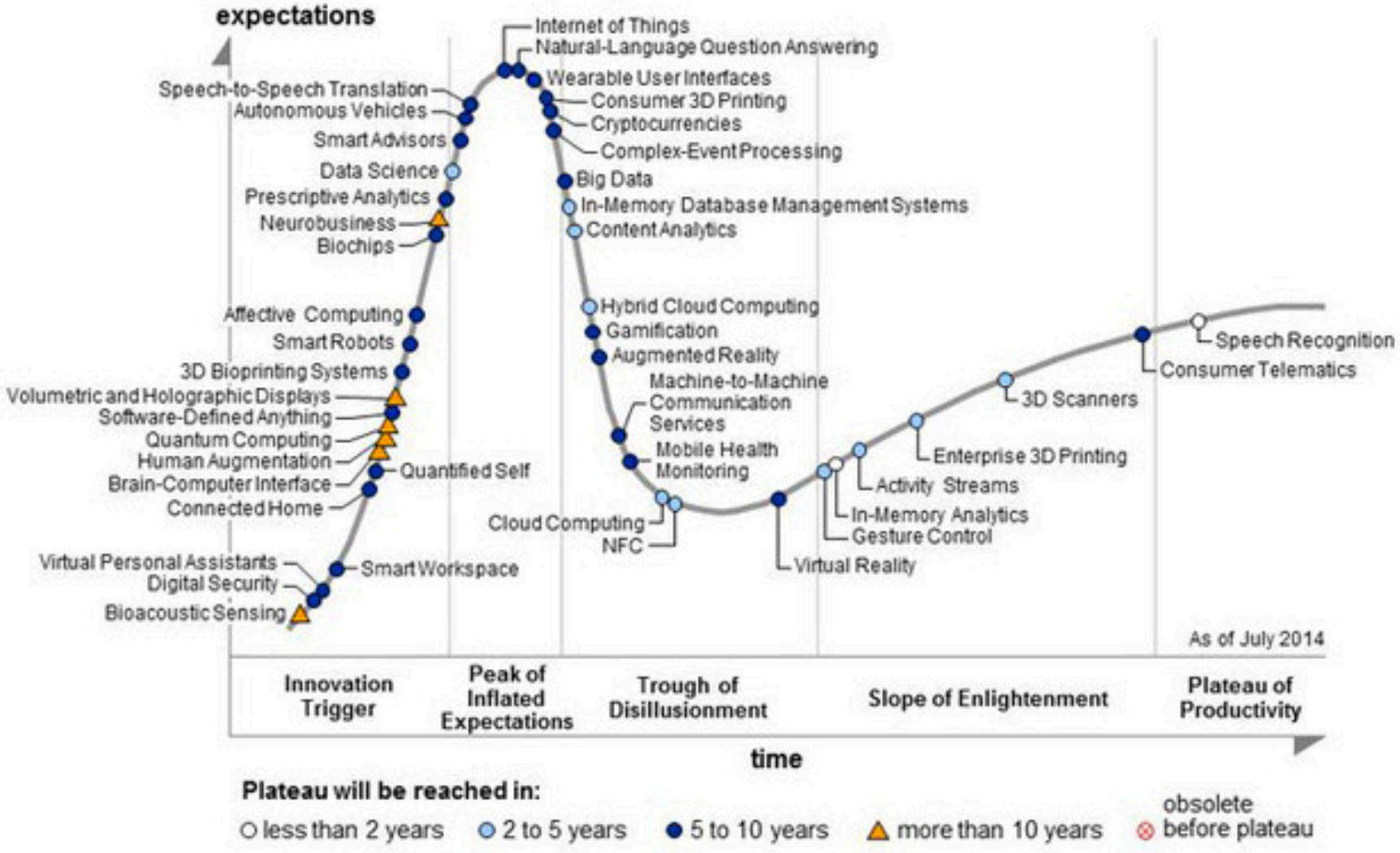
- **A mesh of devices and sensors throughout your daily life**
- **A mesh of devices and sensors throughout the manufacturing environment**
- **A mesh of devices monitoring everything**

Cisco Framework



Source: Cisco IBSG projections, UN Economic & Social Affairs http://www.un.org/esa/population/publications/longrange2/WorldPop2300final.pdf

Peak Hype


expectations
Internet of Things
Natural-Language Question Answering
Wearable User Interfaces
Consumer 3D Printing
Cryptocurrencies
Complex-Event Processing
Big Data
In-Memory Database Management Systems
Content Analytics
Hybrid Cloud Computing
Gamification
Augmented Reality
Machine-to-Machine Communication Services
Mobile Health Monitoring
Cloud Computing
NFC
Virtual Reality
In-Memory Analytics
Gesture Control
Activity Streams
Enterprise 3D Printing
3D Scanners
Speech Recognition
Consumer Telematics
Speech-to-Speech Translation
Autonomous Vehicles
Smart Advisors
Data Science
Prescriptive Analytics
Neurobusiness
Biochips
Affective Computing
Smart Robots
3D Bioprinting Systems
Volumetric and Holographic Displays
Software-Defined Anything
Quantum Computing
Human Augmentation
Brain-Computer Interface
Connected Home
Quantified Self
Virtual Personal Assistants
Digital Security
Bioacoustic Sensing
Smart Workspace
As of July 2014
Innovation Trigger
Peak of Inflated Expectations
Trough of Disillusionment
Slope of Enlightenment
Plateau of Productivity
time
Plateau will be reached in:
less than 2 years
2 to 5 years
5 to 10 years
more than 10 years
obsolete before plateau

IoT 2016

- Gartner says that 6,400,000,000 IoT things were online in 2016, 30% over 2015.

Table 1: Internet of Things Units Installed Base by Category (Millions of Units)

Category	2014	2015	2016	2020
Consumer	2,277	3,023	4,024	13,509
Business: Cross-Industry	632	815	1,092	4,408
Business: Vertical-Specific	898	1,065	1,276	2,880
Grand Total	**3,807**	**4,902**	**6,392**	**20,797**

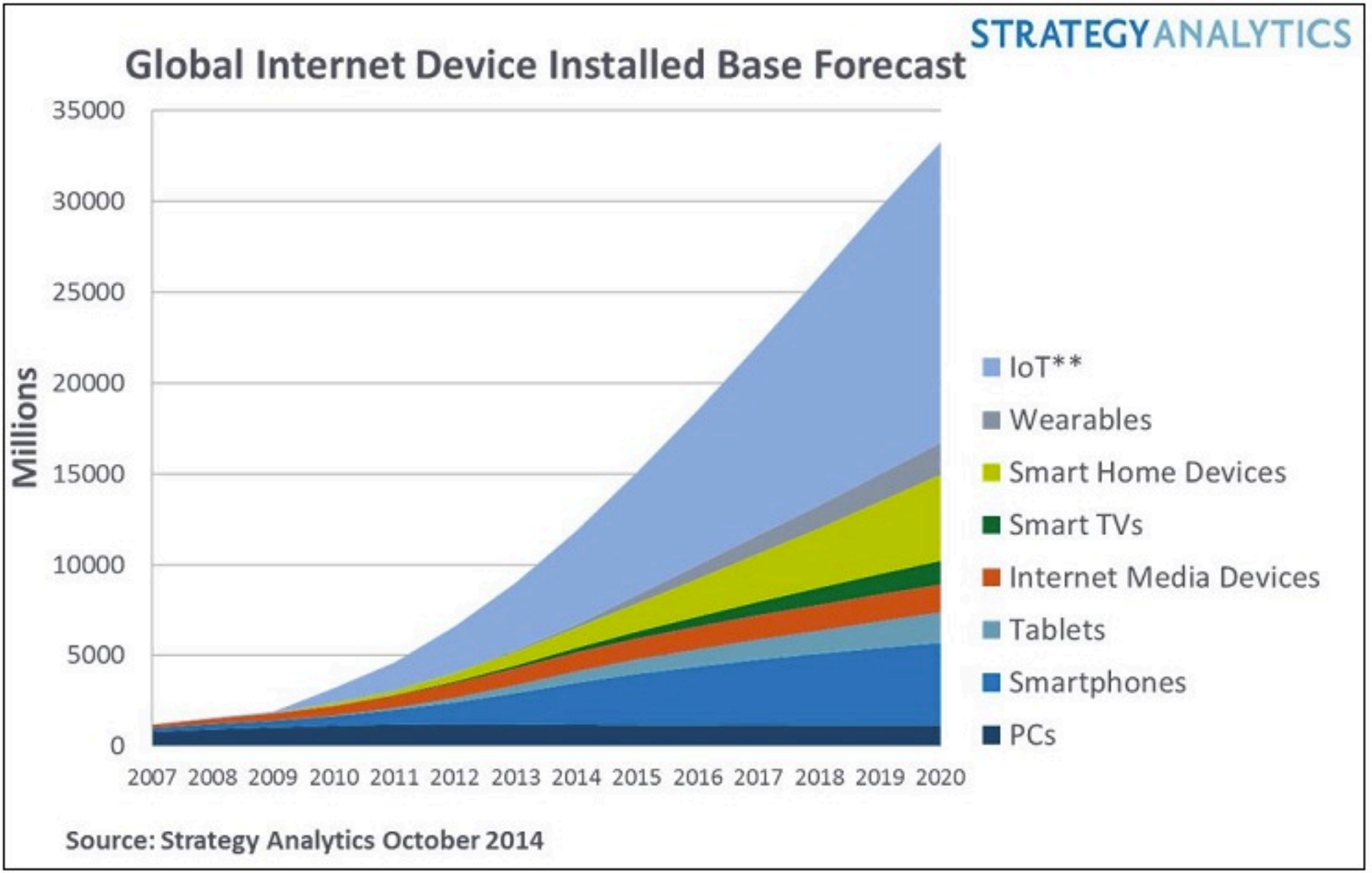
Source: Gartner (November 2015)

IoT 2020

- Gartner predicts 20.8 billion IoT devices online in 2020.

- Spending on "things" in 2015 was $235 billion.

33 Billion Internet Devices By 2020: Four Connected Devices for Every Person in the World, Says Strategy Analytics



IoT Scenario

- A collection of raspberry pi's has been turned over to you to analyze.
- The investigator does not know what they were used for. They saw them and took them all.

- You should fill out an evidence handling sheet.

Use Vbox to add a USB Drive

- Mount the drive using RO as a pass through USB Device in Vbox.

Look for new disk

```
[root@localhost mnt]# dmesg | grep sdb
[  172.439399] sd 3:0:0:0: [sdb] 15351808 512-byte logical blocks: (7.86 GB/7.32
 GiB)
[  172.449550] sd 3:0:0:0: [sdb] Write Protect is off
[  172.449553] sd 3:0:0:0: [sdb] Mode Sense: 00 00 00 00
[  172.459895] sd 3:0:0:0: [sdb] Asking for cache data failed
[  172.459899] sd 3:0:0:0: [sdb] Assuming drive cache: write through
[  172.532687]  sdb: sdb1 sdb2 < sdb5 sdb6 > sdb3
[  172.582129] sd 3:0:0:0: [sdb] Attached SCSI removable disk
[  174.318235] EXT4-fs (sdb3): mounted filesystem with ordered data mode. Opts:
(null)
[  174.700185] FAT-fs (sdb5): Volume was not properly unmounted. Some data may b
e corrupt. Please run fsck.
[  196.743619] EXT4-fs (sdb6): recovery complete
[  196.759344] EXT4-fs (sdb6): mounted filesystem with ordered data mode. Opts:
(null)
[root@localhost mnt]#
```

Look at partitions

```
[root@localhost mnt]# fdisk -l /dev/sdb
Disk /dev/sdb: 7.3 GiB, 7860125696 bytes, 15351808 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x0009a70f

Device     Boot    Start      End  Sectors  Size Id Type
/dev/sdb1           8192  1685546  1677355  819M  e W95 FAT16 (LBA)
/dev/sdb2        1687552 15286271 13598720  6.5G 85 Linux extended
/dev/sdb3       15286272 15351807    65536   32M 83 Linux
/dev/sdb5        1695744  1818623   122880   60M  c W95 FAT32 (LBA)
/dev/sdb6        1826816 15286271 13459456  6.4G 83 Linux

Partition table entries are not in disk order.
[root@localhost mnt]#
```

Hints

- **The system is a debian variant.**
  - use dpkg --admindir=…
- **These were used by developers**
  - These may have custom software installed.

Hints

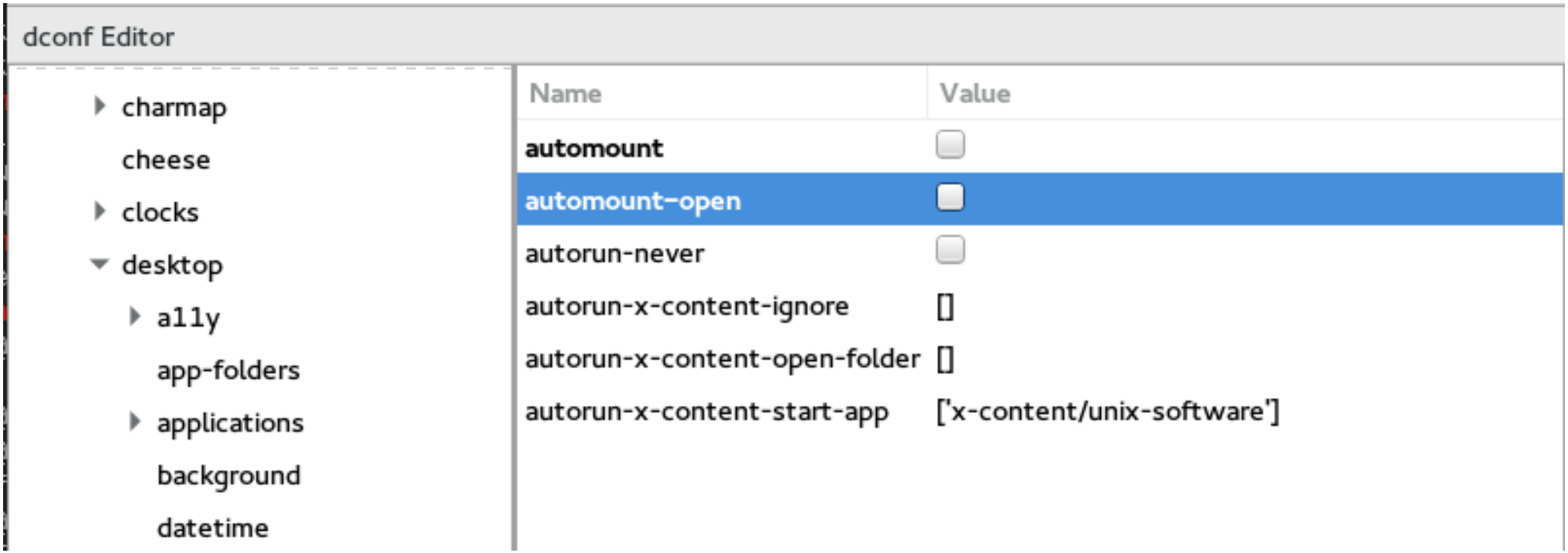
- **If you see only one partition then the system has not been installed.**

```
[root@localhost 0403-0201]# fdisk -l /dev/sdb
Disk /dev/sdb: 7.3 GiB, 7860125696 bytes, 15351808 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x00000000

Device     Boot Start      End  Sectors  Size Id Type
/dev/sdb1        8192 15351807 15343616  7.3G  b W95 FAT32
[root@localhost 0403-0201]#
```

Hints: Disable Auto Mount

- **yum install dconf-editor**
- **dconf-editor**
- **org -> desktop -> media-handling**



Hints: Speed Up

- **Have one person use dclfdd to image the disk, share the copy with each member of the team.**

Hints: Image of entire disk

- **Physical disks can have multiple partitions.**
- **If a DD image was made of a physical disk, you cannot mount it using mount. It doesn't know what partition to mount.**

Hint: Disk Image

- **Use fdisk to display partitions.**

```
[root@localhost UNTITLED]# fdisk -l iot-devkit-201510010757-mmcblkp0-galileo.dir
ect
Disk iot-devkit-201510010757-mmcblkp0-galileo.direct: 1.3 GiB, 1417675776 bytes,
 2768898 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x000a27ad

Device                                          Boot  Start     End Sectors  Si
ze Id Type
iot-devkit-201510010757-mmcblkp0-galileo.direct1 *      2048  106495  104448   5
1M 83 Linux
iot-devkit-201510010757-mmcblkp0-galileo.direct2      106496 2768895 2662400  1.
3G 83 Linux
```

Create loopback devices

- **Use kpartx to create loopback devices for the partitions.**

```
[root@localhost UNTITLED]# kpartx -av iot-devkit-201510010757-mmcblkp0-galileo.d
irect
add map loop0p1 (253:2): 0 104448 linear /dev/loop0 2048
add map loop0p2 (253:3): 0 2662400 linear /dev/loop0 106496
[root@localhost UNTITLED]#
```

Mount images

- **Create mountpoints and mount.**

```
[root@localhost UNTITLED]# mkdir /mnt/p1 /mnt/p2
[root@localhost UNTITLED]# mount -oro /dev/mapper/loop0p1 /mnt/p1
[root@localhost UNTITLED]# mount -oro /dev/mapper/loop0p2 /mnt/p2
[root@localhost UNTITLED]# df -h | grep mnt
/dev/mapper/loop0p1        50M   17M   34M  33% /mnt/p1
/dev/mapper/loop0p2       1.2G  931M  232M  81% /mnt/p2
```

Record information

- **When were last logins?**
- **When was it powered on?**
- **Installed Software?**
- **Disk Size?**
- **MD5?**
- **Make a copy using DCFLDD**

Record information

- **What OS was it?**
- **What IP did it have?**
- **What DNS servers?**
- **Log messages?**
- **Commands?**

Hackathon

- **We know these were used in the hackathon.**
- **Look at their code, what was it supposed to do?**
- **Do you see weaknesses in the code or system that could have been used by attacker**

Assignment

- **Create a python script that will do some forensics function. i.e.**
  - Automount the drive read only and hash everything. With a table of users and times, etc.
  - Create a timeline of system events looking at /var/log/*
  - Create a timeline of file changes
  - Visualize IP Addresses

Assignment

- **Submit a report**
- **Include:**
  - Any vulnerabilities / unapplied patches
  - User accounts
  - Firewall
  - Purpose of application/pi
  - Time of changes
  - Time of attack
  - Evidence handling sheet.