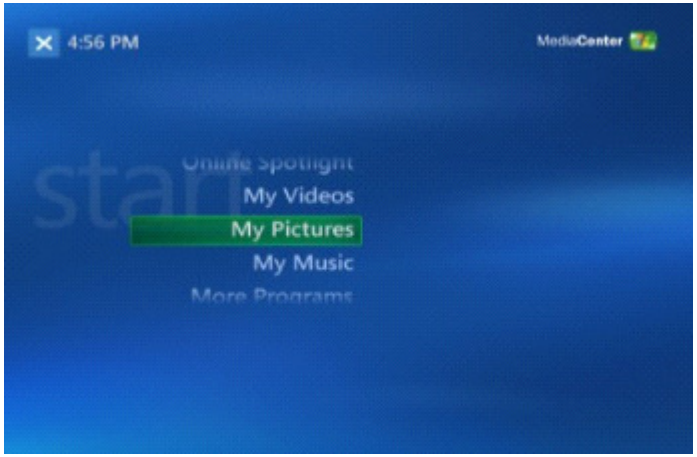
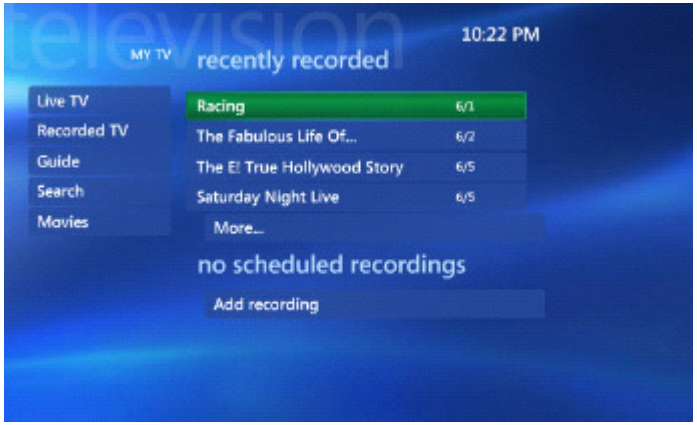
Investigating Microsoft Media Technologies - Xbox

Media Center Extender Capabilities

What is Media Center?





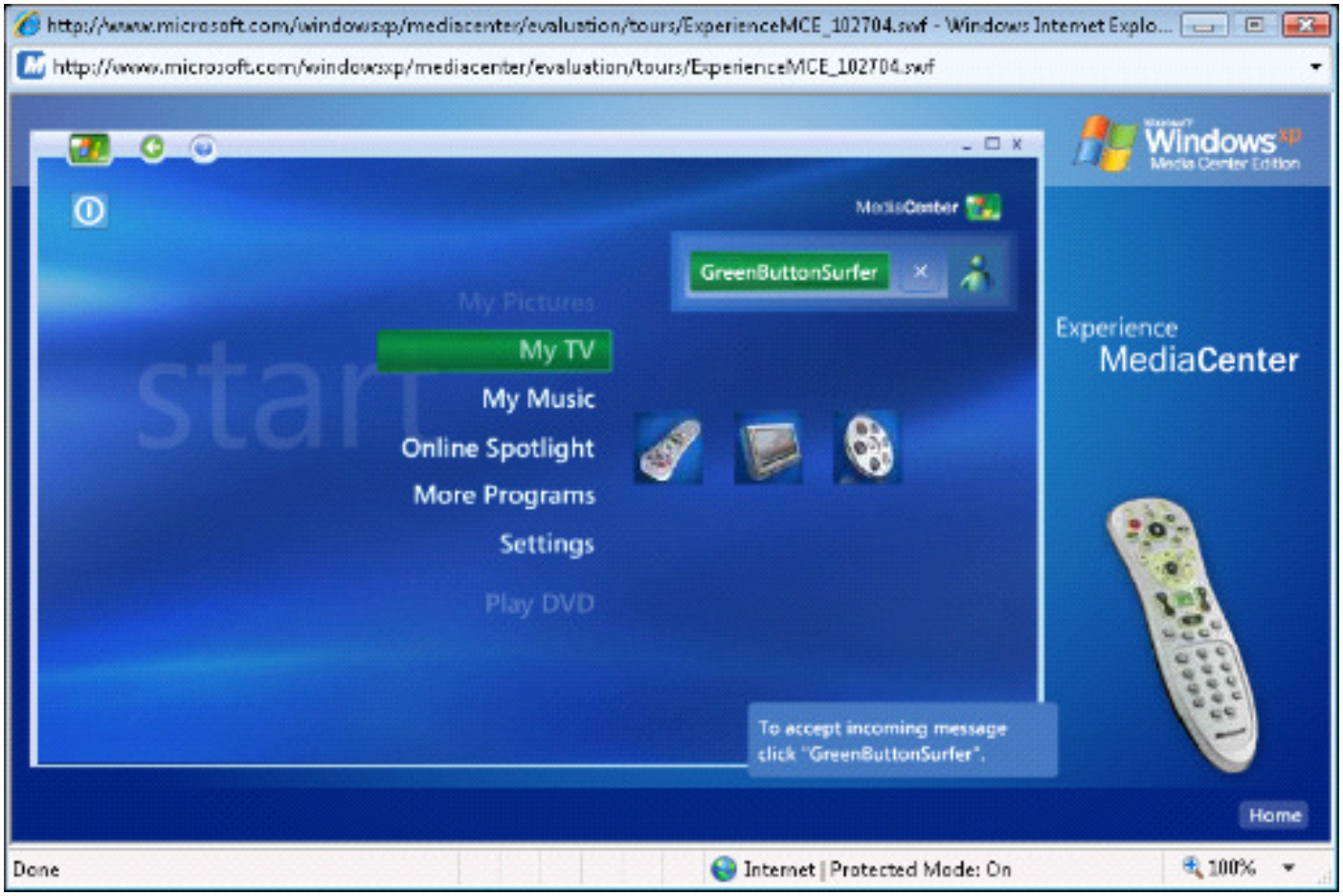
- Available in:
  - Windows XP Media Center Edition
  - Windows Vista Home Premium and Ultimate
- Full computer with addition of Digital Video Recorder
- Additional features

What is Media Center?

- Windows XP Media Center Edition and versions of Vista with MCE feature (Home Premium and Ultimate) are intended to serve as a home entertainment hub
- Only distributed by OEMs
- Very specific hardware requirements to run this version of Windows

What is Media Center?

http://www.microsoft.com/windowsxp/mediacenter/evaluation/tours/default.mspx



Media Center Extender?

- This is software used to "Extend" the Media Center experience:
  - Watch live TV on the extender
  - Watch recorded shows
  - Play music from the Media Center library
  - View pictures from the Media Center library

Media Center Extender?

Media Extender Availability

ORIGINAL XBOX

- Accessory for purchase
- Includes application and remote control

XBOX 360

- Built into the system!
- No need for anything else
  - Recommended that you purchase a MCE remote control

Media Extender Availability

- Additional Hardware Manufacturers are onboard as well:

Media Extender and Xbox

- More so than ever the Xbox gaming console is being integrated into the home entertainment landscape
- These devices (both the OEM extenders and Xbox game consoles) should be considered in any investigation as potential location for evidence

Investigating Microsoft Media Technologies - Xbox

Forensic Examination of the Xbox Gaming Console

Xbox Hard Drive Data

- Downloaded Content from Xbox Live!
- Saved Game Data
- Xbox Live Gamer Profile
- ** Facebook/Twitter/Zune/Last.fm user logon data
- Dashboard Data
- Saved Media (Music/Videos/Photos)

Modded Hard Drive Data

- Anything you would find on a normal PC
  - E-mail
  - Browsing History
  - Chat
  - Pirated Games
  - Etc.

Original Xbox (EEPROM)

- The Serial EEPROM is the key to the Xbox
  - Serial Number of the unit
  - MAC Address of the onboard NIC
  - Hard Drive Key
  - Region Code

Original Xbox (EEPROM)

- The EEPROM also stores a number of settings that are configured during setup…
  - Xbox Live network data
  - Parental control settings
  - Time zone data

Original Xbox Hard Drive

- The Original Xbox hard disk is protected via an mechanism called ATA Security
- ATA Security is a hardware based locking mechanism that uses the EEPROM on the Xbox to store the Hard Drive Key (HDKey)

Original Xbox Hard Drive

- Methods for accessing the drive include:
  - Cable swap: Power up the Xbox and pull the IDE Ribbon and make the connection to the forensic system
  - Hardware logic analyzer physically attached to intercept the ATA password
  - Software logic analyzer to intercept the ATA password
  - "Modded" Xbox to run additional OS provides access to drive data
  - Attacks against the drive's BIOS possible

Original Xbox Hard Drive

- Files system is a modified version of FATX
  - Does maintain MAC data for all files
  - Uses standard file deletion techniques
- There is not native FATX driver so viewing the drive in Windows is not possible
- Versions of the Linux kernel have some FATX capabilities
- *Xbox Original Timestamps are likely wrong***

Original Xbox Hard Drive

Open Console
Boot it up

QUICKLY remove IDE Cable and insert write blocker

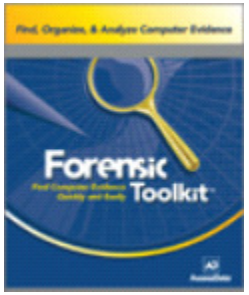


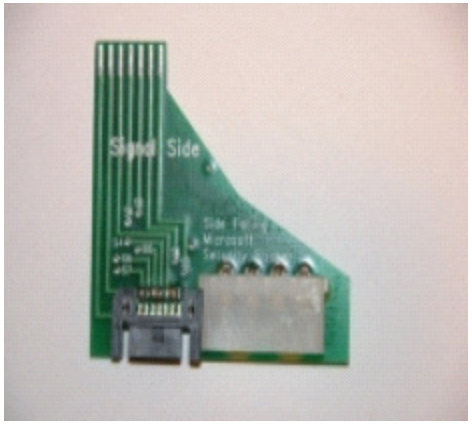
Image drive using your favorite tool

Xbox Memory Cards

- Easiest way to access the data on the memory card is to copy the contents to the Xbox Hard Drive

Accessing the 360 Drive

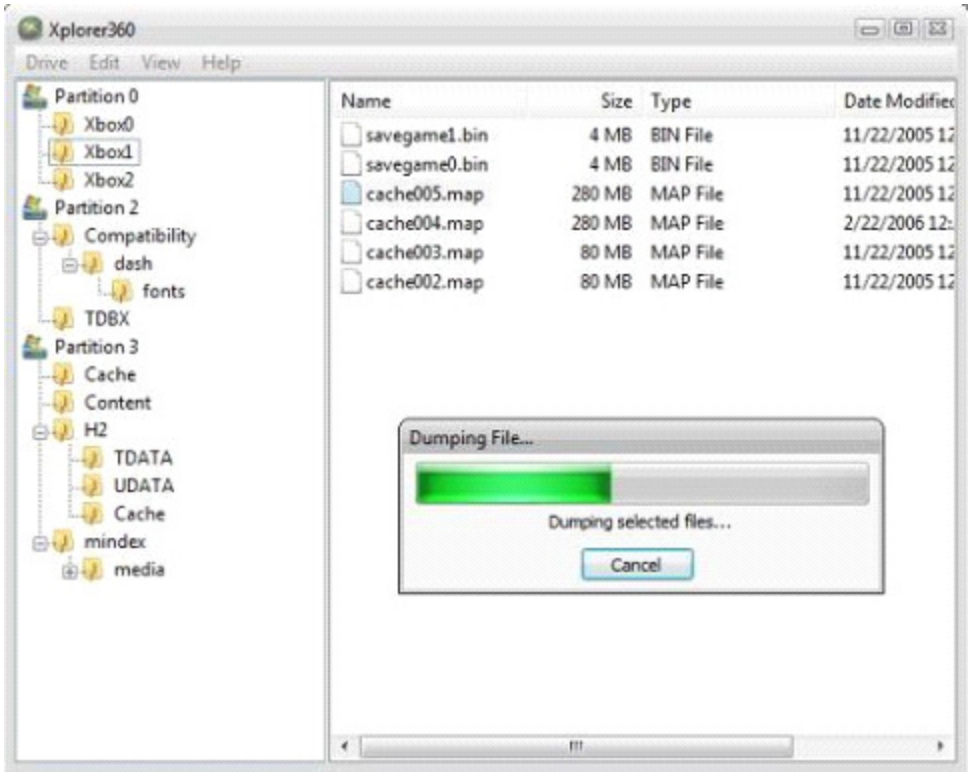
- HD is SATA laptop drive
  - You can take apart drive
  - You can use an adapter
    - http://www.360sata.com/ (site no longer active)
    - Connects to SATA and power without opening HD case
    - Connect to SATA/USB adapter and write blocker




FRED
FireFly™ SATA
Digital Intelligence
Pwr WrBlk Act
800/400
Bilingual

Accessing the 360 Drive

- http://www.360gamesaves.com/
  - Software to access data on 360 HD



Xbox and Xbox 360 Data

- The following data is kept on the local Xbox hard drive and/or memory card:
  - Downloaded content from Xbox Live (Games, Trailers, etc)
  - Saved game data (Progress, Statistics, etc)
  - Xbox Live gamer profile and Gamer Tag pictures

Xbox Hard Drive Partitions

- There are 7 distinct partitions on an Xbox HD
  - Disk configuration partition
  - Game Cache A (temporary game data)
  - Game Cache B (binary data)
  - Game Cache C (buffer.in and fft.in files)

Xbox Hard Drive Partitions

- There are 7 distinct partitions on an Xbox HD (Continued)
  - System Files (System files, dashboard, mod info)
  - Data Files (Saved games, downloaded content, Xbox Live profile)
  - Unused space (could contain Linux code on a "modded" Xbox)

Investigative Impact

- Continue to be aware of the "Modded" Xbox
  - Any data that would be found on a PC
    - E-mails, Chat logs, Browser History, etc
    - Pirated media files and software
    - File access time data for used resources

Additional Resources

- **Xbox security issues and forensic recovery methodology (utilizing Linux),** Chris Vaughan, ScienceDirect-Digital Forensics Online Journal, Volume 1, Issue 3, ppg 165-172
- **Hacking the Xbox: An Introduction to Reverse Engineering**, Andrew Huang, No Starch Press, July 2003
- http://www.xbox-linux.org/wiki/Main_Page
- **Details of the Xbox Hard Drive Locking Mechanism** http://www.xbox-linux.org/docs/hdpassword.html
- **Investigating the Microsoft Xbox 360** Search Training Services, Earl Door, Steven Bolt

Investigating Microsoft Media Technologies - Xbox

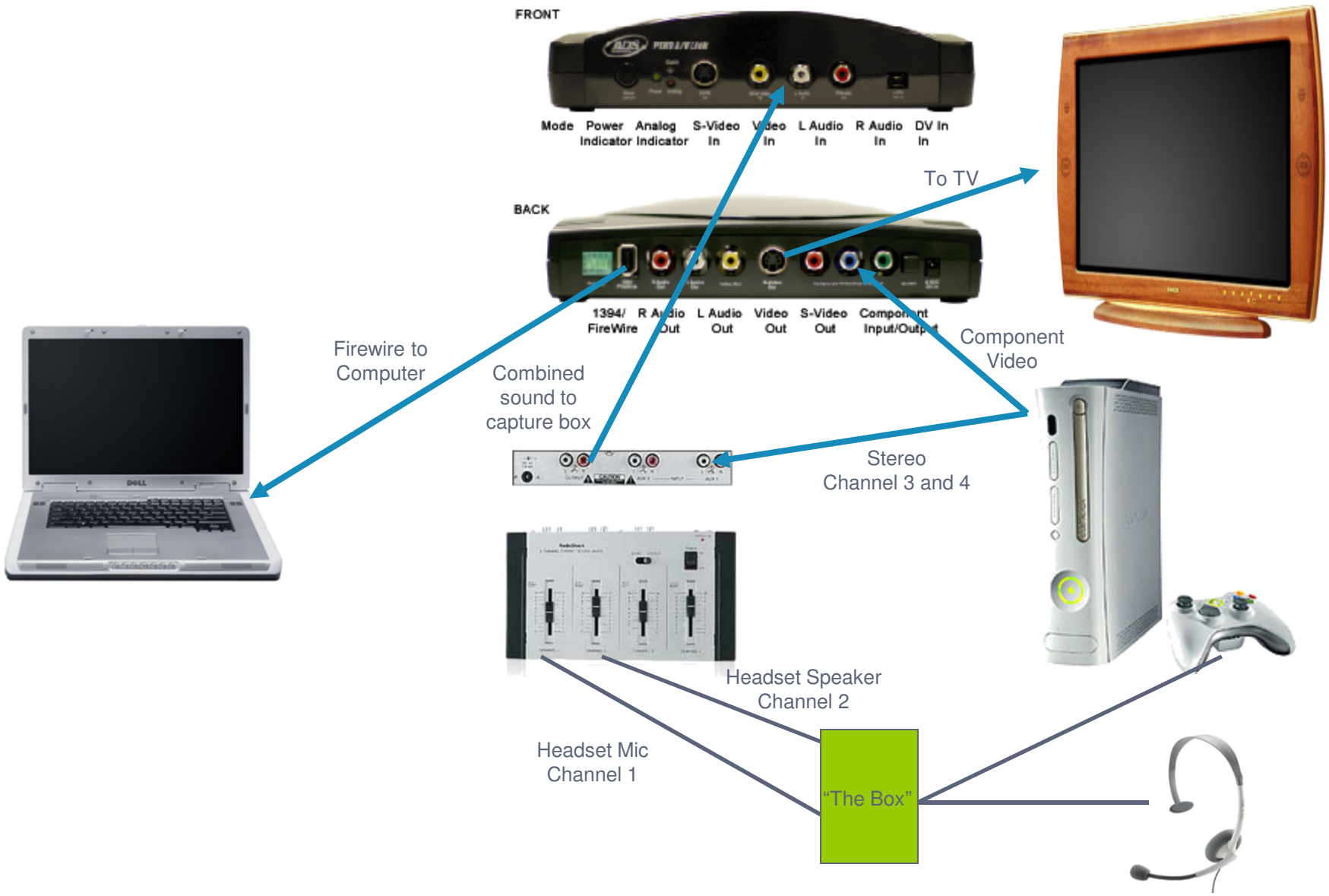
Microsoft Xbox Live! Investigation Rig

Undercover Operations

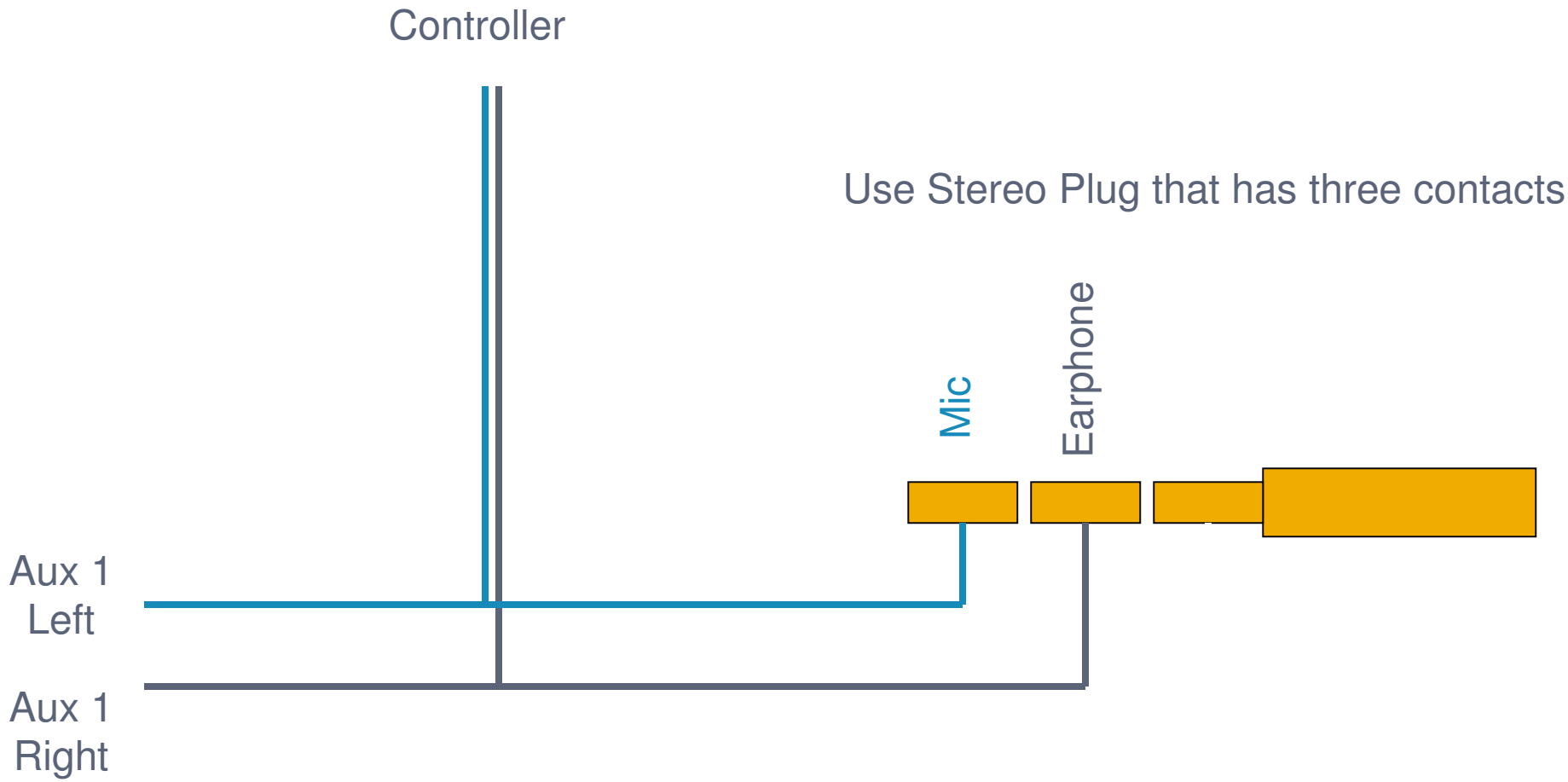
- Investigators may participate in Xbox live in undercover operations
- Video and Audio capture needs to be recorded
- Simple video capture hardware WILL NOT capture voice communications
- Headset audio does not go through system speakers

Prototype Capture Rig

- XBox 360
- Pyro AV capture box
- Computer
- Audio Mixer
- The "Frankenbox" headset splitter
- Goal
  - Record all video, game audio AND player voice communication to computer


FRONT
Mode
Power Indicator
Analog Indicator
S-Video In
Video In
L Audio In
R Audio In
DV In In
BACK
1394/ FireWire
R Audio Out
L Audio Out
Video Out
S-Video Out
Component Input/Output
To TV
Firewire to Computer
Combined sound to capture box
Component Video
Stereo Channel 3 and 4
Headset Speaker Channel 2
Headset Mic Channel 1
"The Box"

The "Frankenbox"



Investigating Microsoft Media Technologies - Xbox

Microsoft Criminal Compliance Can Help

Geek Disclaimer

<GEEK>

- We are **Geeks** and not lawyers so when it comes to legal questions and issue above and beyond this presentation we will be deferring to Microsoft legal counsel.
- Information presented in this delivery has been reviewed by counsel and is **Law Enforcement Sensitive.**
- Contact information for additional information to follow….

</GEEK>

Serving Legal Process

Option 2 = Non-Emergencies

- *This should be the main number for all legal inquires into Microsoft regarding any of the MSN properties including matters involving Xbox Live.*

Serving Legal Process

- Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves "the immediate danger of death or physical injury to any person…" as defined in 18 U.S.C. § 2702(c)(4) and (b)(8).
- Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorist threats, etc.

Serving Legal Process

- Emergency Requests:
  - Send a letter on Official Agency Letterhead- signed and dated
  - Summary of facts, in English, describing the emergency
  - State that there is an emergency "involving immediate danger of death or serious physical injury requiring disclosure of the information without delay."
  - The full name of the requested account (e.g. "robert_compliance@hotmail.com") and what data they are requesting (e.g. "Subscriber Information and IP History").

Serving Legal Process

MSN Services (MSN.com, WebTV, Groups, XBox Live!, IM, etc):

FAX: (425) 727-3490

Microsoft Corporation
Attn: MSN Custodian of Records
One Microsoft Way
Redmond, WA 98052-6399

MSN Hotmail, Passport and Windows Live Mail:

FAX: (650) 693-7061

Microsoft Corporation
Attn: MSN Custodian of Records
1065 La Avenida
Mountain View, CA 94043

Obtaining Additional Information

- All request should be processed through the Microsoft Law Enforcement Portal

  https://www.microsoftlawportal.com

- To request access send mail to leportal@microsoft.com