Forensics in Tribal Gaming

Information Technology Division

Digital Forensics
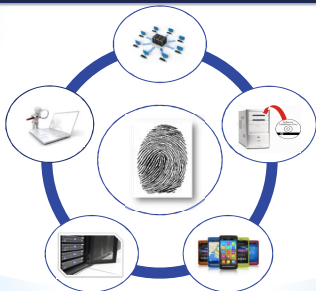
Course Overview

WHAT?	WHY?	WHO?	HOW?
• Common Types • Investigations	• Chain of Custody • Evidence Gathering	• First Responders • Gaming Commissions	• Plan of Action • Collected Evidence

Gaming Forensics

Criminalistics

Video Analysis

Accounting

Gaming Forensics

Common Types

- ❑ Non-existent payline or bonus awards
- ❑ Physical reel strip vs. prize/award mismatch
- ❑ Credit award not present within prize schedule
- ❑ Electromechanical fault (reels continue to spin)
- ❑ External bonus awarded to selected player accounts
- ❑ Physical tampering (electrical shock or interference)
- ❑ Backend system manipulation – new investigating further

Investigative Purpose

Public Trust

MICS 547.5 TGRA chooses ITL for certification

WHAT?

Chain of Custody

Include:
- Inception Evidence Collection
- Paper Trail
- Integrity of evidence until processed
- TGRA &/or Regulatory body determine extent of actions
- Best Practice Guideline
  - US DOJ (Justice) / NIST(National Institute of Standards and Technology

WHY?

Evidence Gathering

HARDWARE & SOFTWARE MANUALS

WHY?

Evidence Gathering

MICS 547.13 Program Storage Media
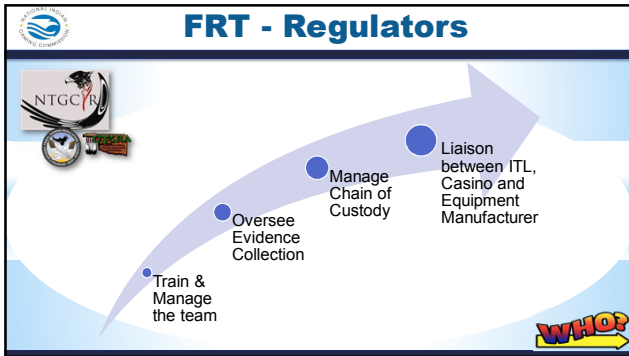

Evidence Gathering

First Responders

Those directly affecting gaming integrity

- ❑Regulators
- ❑Gaming Operations
- ❑Information Technology
- ❑Security
- ❑Surveillance
- ❑Accounting and Auditing

FRT - Regulators

- Train & Manage the team
- Oversee Evidence Collection
- Manage Chain of Custody
- Liaison between ITL, Casino and Equipment Manufacturer

FRT – Gaming Operations

DEPLOY!

Report Findings

Inform Personnel

DO NOT TURN IT ON, OR ON IF OFF

findings regulatory body(s)

FRT – Information Technology

Report Findings

Backend System Logs

Remote Access System Logs

Accounting System Error Logs

MICS 547.3 Responsibility for technology

FRT - Security

Report Findings

MICS 547.5 TGRA responsible for security

WHO?

FRT - Surveillance

Con... ...eillance
C... ...o of
Cov... ...llection

Report Findings

MICS 543.21 Surveillance

WHO?

FRT – Accounting & Audit

Report Findings

Casino Management System

MICS 547.8(2)(k) Critical Memory gain (i) Accounting data
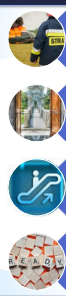
WHO?

Gaming Commission

As the regulatory body submits information and components for a forensic examination following a thorough investigation and gathering of information and evidence.

WHO?

Plan of Action
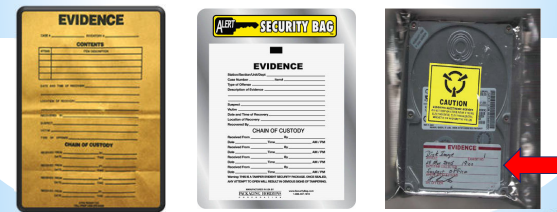
First Responder Team

Forensic Threshold

Escalation

Readiness Training

HOW?

Collected Evidence

Must be secured and stored in a controlled environment

HOW?

Collected Evidence

Areas of concern for gaming operators are:

➢ Game malfunction for server connected/controlled games (SBG, Server Supported, etc.)
➢ Verification of Jackpots (Server level vs. terminal level)
➢ Patron disputes over game outcomes
➢ "Superuser" type accounts on the player tracking side
➢ Gaming Equipment or Host Server tampering
➢ Disgruntled Manufacturers and internal/external (vendor's) IT employees

Risk Mitigation

Risks factors YOU can control:

➢ **Licensure**: Vetting vendors who have remote access
➢ **Internal user accounts**: does one person have too many access rights (who watches the watchers?)
➢ **Tape Seal management**: Are all appropriate areas sealed up? Are all seals tracked/accounted for?
➢ **Proper accounting/reconciliation**: are there any detectable patterns or abnormal behaviors (runaway meters, mismatch to indicate theft, etc.)?

WIIFM?

➢ Understand how to identify when a forensic occurs
➢ Familiarize yourself with the common types to assist with addressing
➢ Have a Plan of Action for Forensic events/investigations
➢ Know your First Responder Team and contact information
➢ Always review protocols and understand your Risks

Questions

Tim Cotton	Jeran Cox	Michael Curry
IT Auditor	IT Auditor	IT Auditor
timothy_cotton@nigc.gov	jeran_cox@nigc.gov	michael_curry@nigc.gov

Sean Mason	Travis Waldo
IT Auditor	Director, IT
sean_mason@nigc.gov	travis_waldo@nigc.gov