

IT-107 Gaming Forensics Participant Guide

IT-107 Gaming Forensics



Information Technology Division

KEY POINTS

IT-107 Gaming Forensics Participant Guide



Digital Forensics



KEY POINTS

1. Network Forensics
2. Computers
3. Mobile Devices
4. Database
5. Live

IT-107 Gaming Forensics Participant Guide



Course Overview

WHAT?

- Common Types
- Investigations

WHY?

- Chain of Custody
- Evidence Gathering

WHO?

- First Responders
- Gaming Commissions

HOW?

- Plan of Action
- Collected Evidence

KEY POINTS

IT-107 Gaming Forensics Participant Guide

Has anyone gone through a forensic with an ITL?

Yes

No

Start the presentation to activate live content

If you see this message in presentation mode, install the add-in or get help at [PollEv.com/app](https://www.polleverywhere.com/app)

KEY POINTS

Poll Title: Has anyone gone through a forensic with an ITL?

https://www.polleverywhere.com/multiple_choice_polls/TV3tvEM9ndVGHB9

IT-107 Gaming Forensics Participant Guide



Gaming Forensics



Criminalistics



Video Analysis



Accounting

KEY POINTS

1. Criminalistics are the study and collection of physical evidence at the crime.
2. Video Analysis is the scientific study and collection of video for legal matters.
3. Accounting is the study and analysis of collection of financial evidence.

IT-107 Gaming Forensics Participant Guide



Gaming Forensics



KEY POINTS

In the regulated gaming arena, a forensic investigation typically occurs when gaming or associated equipment has malfunctioned or performed an operation outside the range of that equipment's programmed abilities

IT-107 Gaming Forensics Participant Guide



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



KEY POINTS

IT-107 Gaming Forensics Participant Guide



Investigative Purpose

Public Trust

MICS 547.5 TGRA chooses ITL for certification



KEY POINTS

Why are forensic investigations and relevant procedures important?

- For instituting a set of operational forensic procedures regarding security of evidence
- For establishing communication and proper procedures between the regulatory bodies, operators, and independent testing laboratories
- To help in maintaining service and continuity between gaming departments by isolating the incident
- For recognizing, investigating and responding to incidents. This will also help with mitigating future risks!
- Maintaining public trust (damage control!)

IT-107 Gaming Forensics Participant Guide



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?

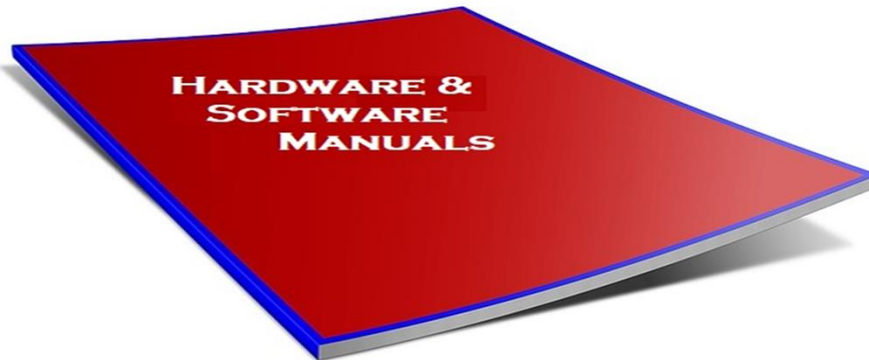
KEY POINTS

Chain of Custody is vital in the event that a dispute goes to court.

IT-107 Gaming Forensics Participant Guide



Evidence Gathering



WHY?

KEY POINTS

Examples of physical/non-electronic evidence include:

- Ticket cash receipts and jackpot/regular vouchers
- Photographs of gaming and associated equipment
- Gaming Machine/Terminal cabinet
- Machine Entry Authorization Log Book (MEAL Book) and Progressive Entry Authorization Logs (PEAL)
- Key Control logs

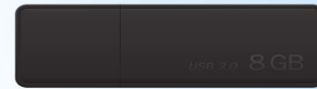
Examples of physical/non-electronic evidence include:

- Miscellaneous handwritten notes (for example, comments written down during previous service)
- Player Promotional Cards
- Tools possibly used to compromise the gaming equipment (screwdrivers, rods, magnets, taser, etc.)
- Hardware and software manuals
- Server/System Generated Reports (Door Entry, Metering, etc.)

IT-107 Gaming Forensics Participant Guide



Evidence Gathering



MICS 547.13 Program Storage Media



KEY POINTS

Examples of electronic evidence include:

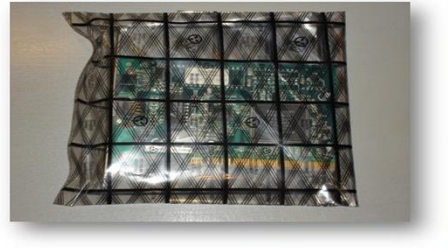
- Hard drive/Hard drive data
- CDs, DVDs, or other optical storage devices
- USB Flash Drives, Compact Flash cards, or other flash memory storage devices
- Wireless Devices
- EPROMs with or without logic boards

Incidents may not involve gaming equipment, but other parts of the gaming floor. Evidence associated with these incidents include:

IT-107 Gaming Forensics Participant Guide



Evidence Gathering



KEY POINTS

Have a “crash cart”

Protect yourself and equipment from static discharge.



First Responders

Those directly affecting gaming integrity

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



KEY POINTS

IT-107 Gaming Forensics Participant Guide

Does anyone have a first Responders Team?

Yes

No

Working on it

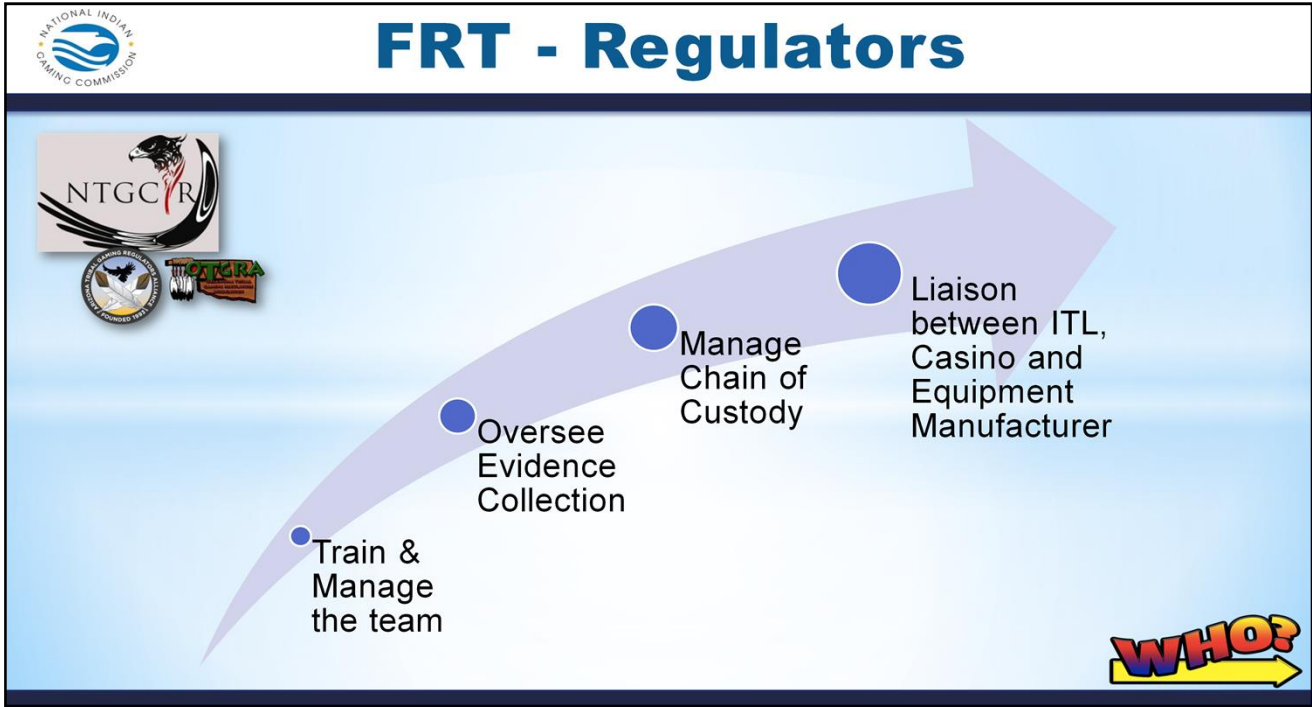
Start the presentation to activate live content
If you see this message in presentation mode, install the add-in or get help at PollEv.com/app

KEY POINTS

Poll Title: Does anyone have a first Responders Team?

https://www.polleverywhere.com/multiple_choice_polls/ifosYLx4hEXGFBB

IT-107 Gaming Forensics Participant Guide



KEY POINTS

IT-107 Gaming Forensics Participant Guide

The diagram is titled "FRT - Gaming Operations" and features the National Indian Gaming Commission logo in the top left. A central white cloud contains the text "Report Findings". To the left of the cloud is a red button labeled "DEPLOY!". To the right is a grey button labeled "IDENTIFY". Below the cloud are three blue boxes: the left one says "Inform Personnel", the middle one says "DO NOT TURN IT OFF, OR ON IF OFF", and the right one says "Report Findings Regulatory Body(s)". A "WHO?" graphic with a yellow arrow is in the bottom right corner.

KEY POINTS

DO NOT TURN IT OFF IF ON, OR ON IF OFF

IT-107 Gaming Forensics Participant Guide



FRT - Security



MICS 547.5 TGRA Responsible for Security



KEY POINTS

The Security Department are the people oriented investigation and enforcement expert on the scene and are responsible for:

IT-107 Gaming Forensics Participant Guide

FRT - Surveillance

Concept
Coverage
Coverage

Report Findings

Surveillance
Department of

MICS 543.21 Surveillance

WHO?

KEY POINTS

The Surveillance Department are the ever present “eye in the sky” and are responsible for maintaining constant coverage.

IT-107 Gaming Forensics Participant Guide



FRT – Accounting & Audit



Report Findings

Casino
Management
System

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



KEY POINTS

The Auditing and Accounting Department are the money experts and are responsible for examining tickets.

IT-107 Gaming Forensics Participant Guide



Gaming Commission



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



KEY POINTS

IT-107 Gaming Forensics Participant Guide



Plan of Action



First Responder Team



Forensic Threshold



Escalation



Readiness Training

HOW?

KEY POINTS

What should a forensic plan of action consist of?

- Establishing a First Responder Team?
- Establishing a Forensic Threshold?
- Escalation guidelines?
- Forensic Readiness Training?

IT-107 Gaming Forensics Participant Guide



Collected Evidence

Must be secured and stored in a controlled environment

EVIDENCE

CASE # _____ INVENTORY # _____

CONTENTS

ITEM	ITEM DESCRIPTION

DATE AND TIME OF RECOVERY _____

LOCATION OF RECOVERY _____

RECEIVED BY _____

SUSPECT _____

VICTIM _____

TYPE OF OFFENSE _____

CHAIN OF CUSTODY

RECEIVED FROM	DATE	TIME

ALERT SECURITY BAG

EVIDENCE

Station/Section/Unit/Dept _____
Case Number _____ Item# _____
Type of Offense _____
Description of Evidence _____

Suspect _____
Victim _____
Date and Time of Recovery _____
Location of Recovery _____
Received By _____

CHAIN OF CUSTODY

Received From	By	Time	AM / PM

MANUFACTURED IN USA BY
PACKAGING HORIZONS
www.SecurityBags.com 1-888-487-1919



HOW?

KEY POINTS

The transfer from evidence collection to a lab should follow procedures such as:

- Proper packaging
- Shipping
- Evidence Repository
- Line of Communication
- Red Arrow reiterate how much date/time signature of individual(s) and proper chain of custody

IT-107 Gaming Forensics Participant Guide



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



KEY POINTS



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.)?

KEY POINTS

IT-107 Gaming Forensics Participant Guide



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

KEY POINTS

IT-107 Gaming Forensics Participant Guide



Questions

Tim Cotton

IT Auditor

timothy_cotton@nigc.gov

Jeran Cox

IT Auditor

jeran_cox@nigc.gov

Michael Curry

IT Auditor

michael_curry@nigc.gov

Sean Mason

IT Auditor

sean_mason@nigc.gov

Travis Waldo

Director, IT

travis_waldo@nigc.gov

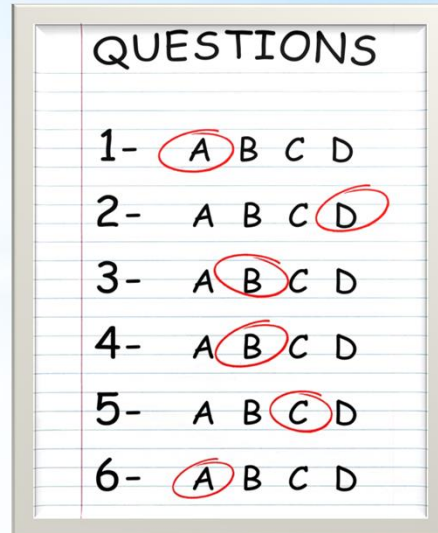
KEY POINTS

IT-107 Gaming Forensics Participant Guide



Knowledge Review

- Be sure to include your name and email address
- Do your best
- Be on the lookout for the survey email 90 days from today



KEY POINTS

IT-107 Gaming Forensics Participant Guide

FY2018 RGT Knowledge Review Day 2
When survey is active, respond at [PolleEv.com/nigc](https://www.polleverywhere.com/nigc)

0 surveys done
0 surveys underway

Start the presentation to see live content. Still no live content? Install the app or get help at [PolleEv.com/app](https://www.polleverywhere.com/app)

Poll Title: FY2018 RGT Knowledge Review Day 2

<https://www.polleverywhere.com/surveys/1Lr00Qis1>



Course Evaluation

- Provide an honest assessment of your experience
- Written suggestions and comments are greatly appreciated and allow us to improve your experience



KEY POINTS

IT-107 Gaming Forensics Participant Guide



Course Eval IT-107 Forensics in Gaming
When survey is active, respond at [PollEv.com/nigc](https://www.poll Everywhere.com/nigc)





Start the presentation to activate live content
If you see this message in presentation mode, install the add-in or get help at [PollEv.com/app](https://www.poll Everywhere.com/app)
0 surveys underway



KEY POINTS

Poll Title: Course awe34r567u8i9o0p-[\

IT-107 Forensics in Gaming

<https://www.polleverywhere.com/surveys/ZmhFBzBoc>