

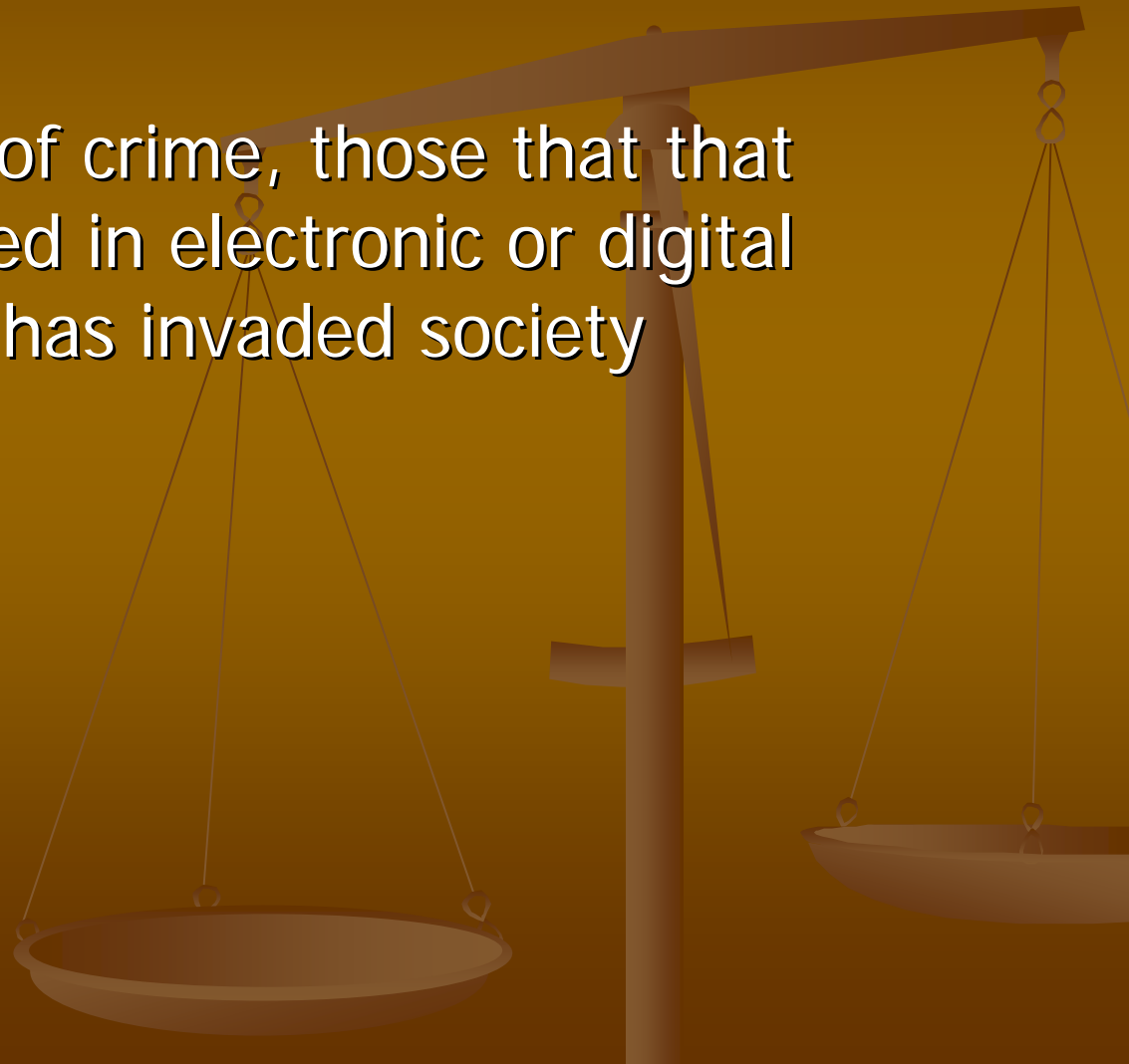
Investigations in the Digital Age

Bill Oettinger



Digital Investigations

A new class of crime, those that are committed in electronic or digital arenas, has invaded society



No Computer System Safe

- California v Grace, Wilson (2000)
- Michael McKeivitt



Digital Transmission

- World Trade Center Attacks
 - Ramsey Yousef
 - Zacarias Moussaoui



Digital Transmission

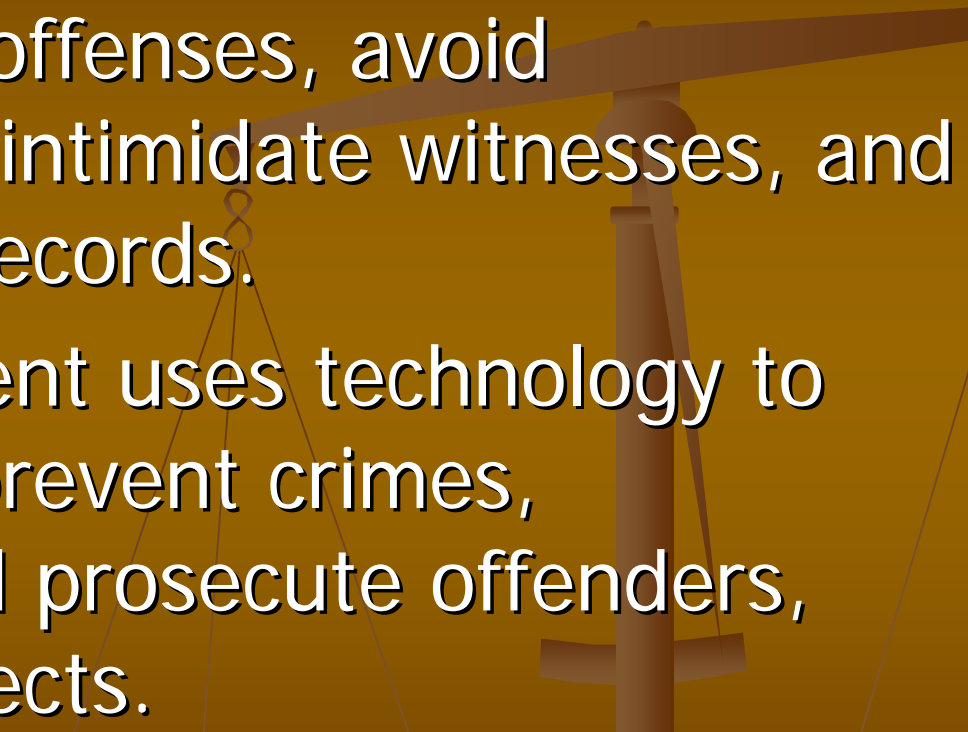
- Daniel Pearl

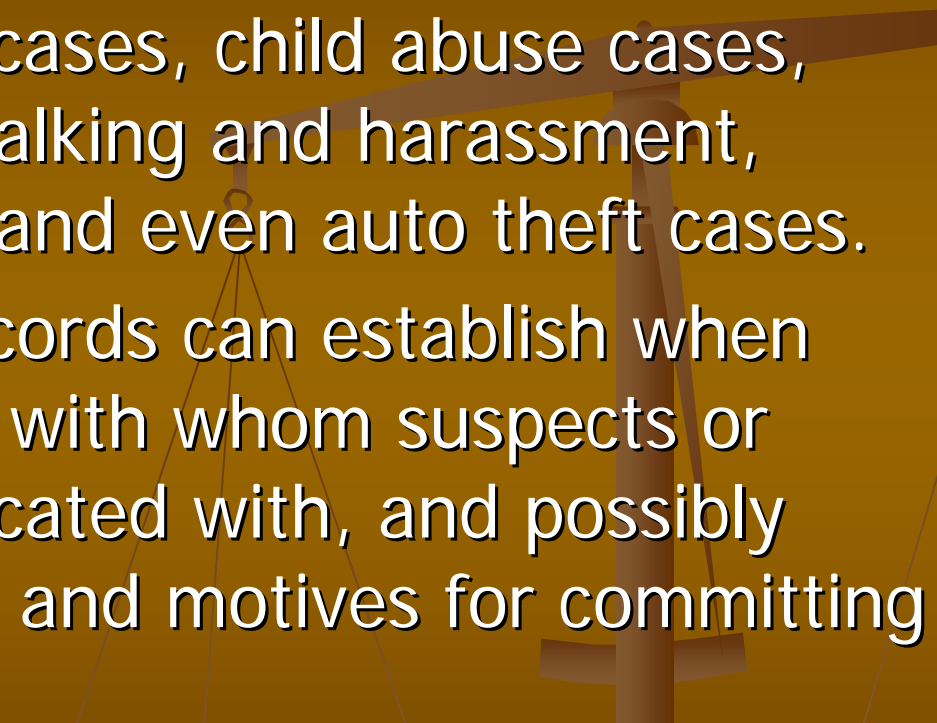


Digital Transmission

- Enron - Didn't shred enough



- 
- Criminals are using technology to facilitate their offenses, avoid apprehension, intimidate witnesses, and change court records.
 - Law enforcement uses technology to solve crimes, prevent crimes, apprehend and prosecute offenders, eliminate suspects.

- 
- Digital evidence can be useful in homicides, missing persons cases, child abuse cases, drug offenses, stalking and harassment, frauds, ID theft, and even auto theft cases.
 - Computerized records can establish when events occurred, with whom suspects or victims communicated with, and possibly show their intent and motives for committing a crime.

Digital Data

- PDA
- Cell Phones
- Laptops
- Portable Drives
- X-Boxes
- Motor Vehicles



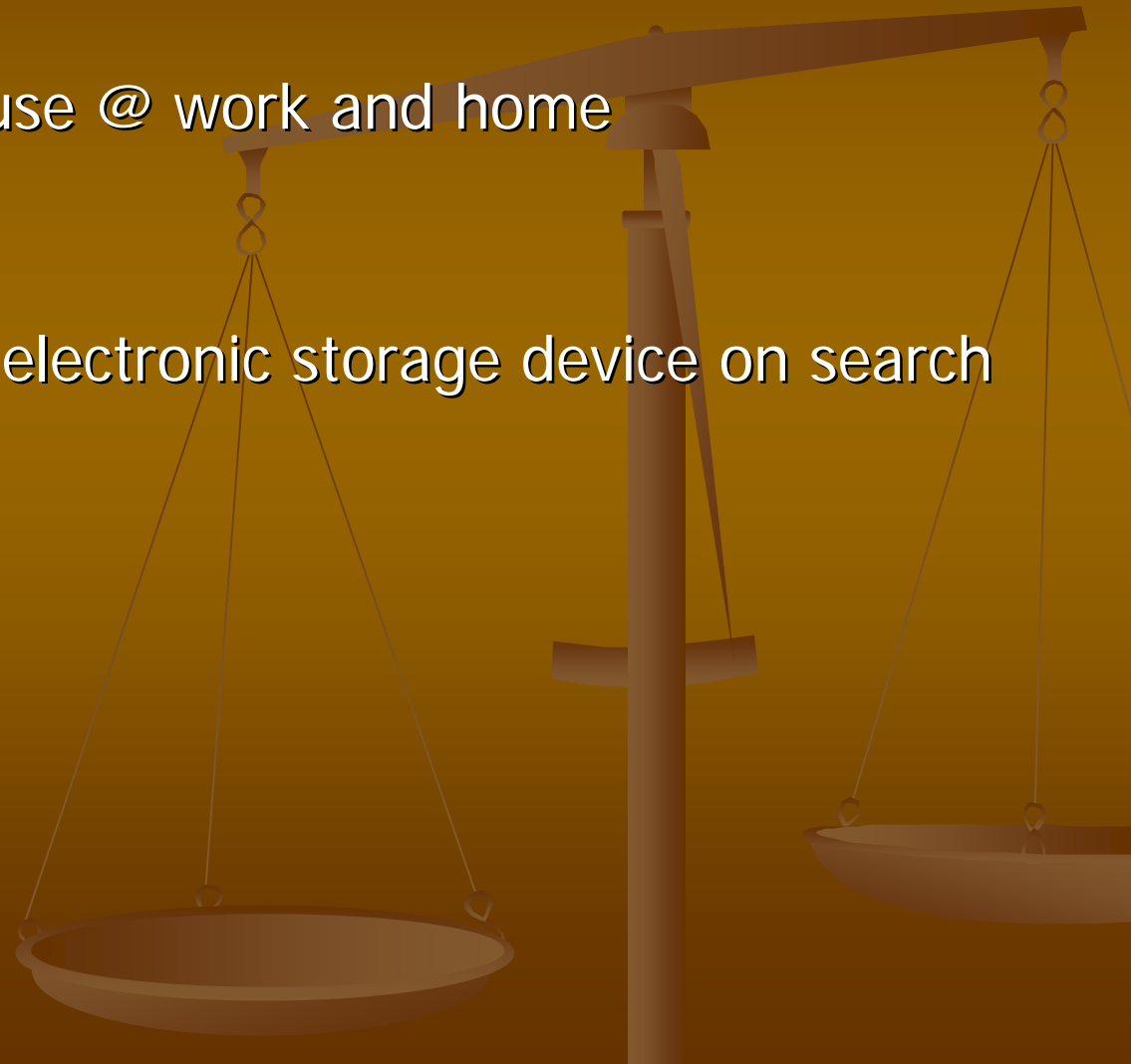
Digital Data

Civil

Employee computer use @ work and home

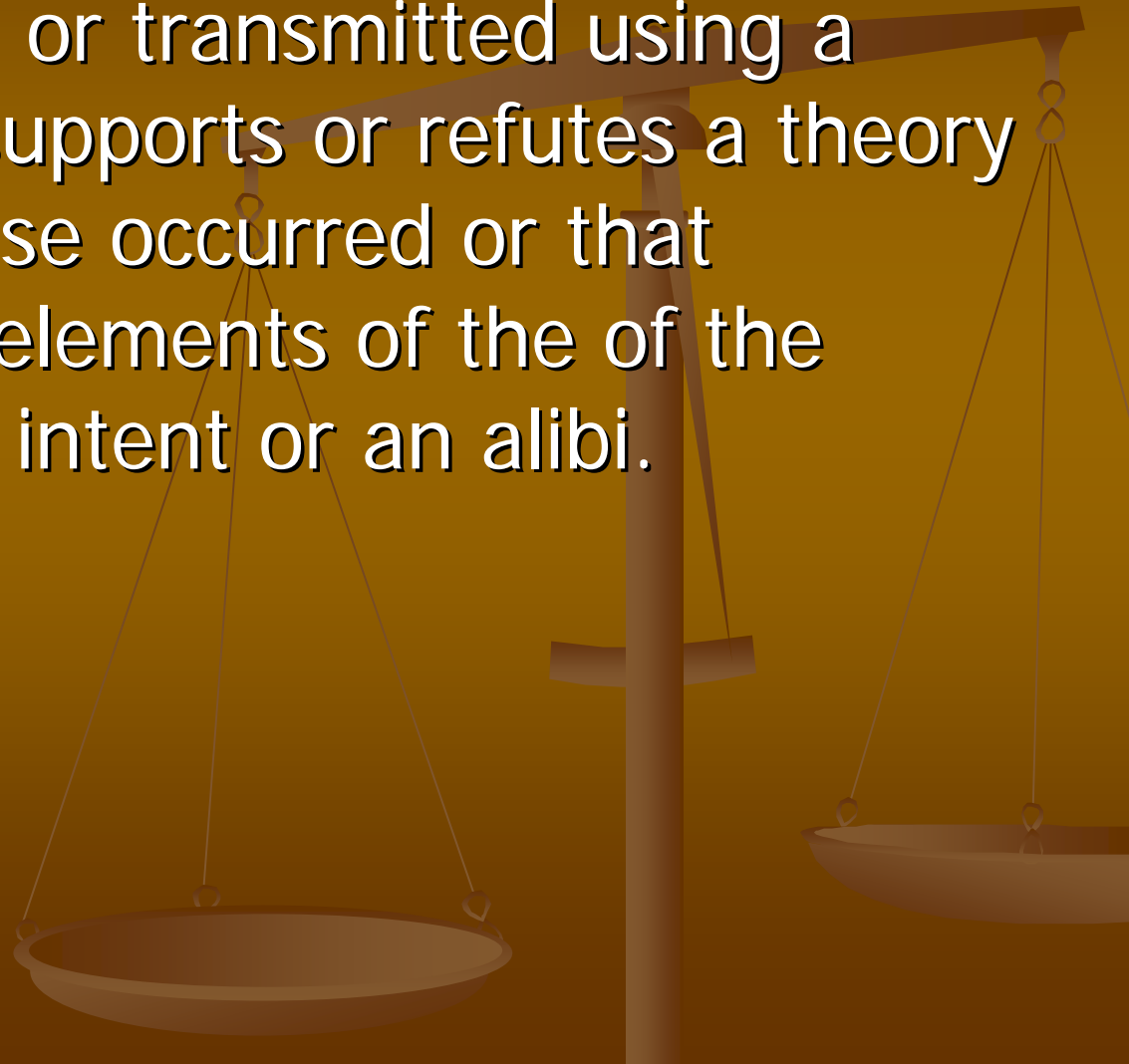
Criminal

Include language for electronic storage device on search warrants



Definition of digital evidence

- Any data stored or transmitted using a computer that supports or refutes a theory of how an offense occurred or that address critical elements of the offense such as intent or an alibi.



Sources of Digital Evidence



Open Computer Systems

Communication Systems

Embedded Computer Systems

Open Computer Systems

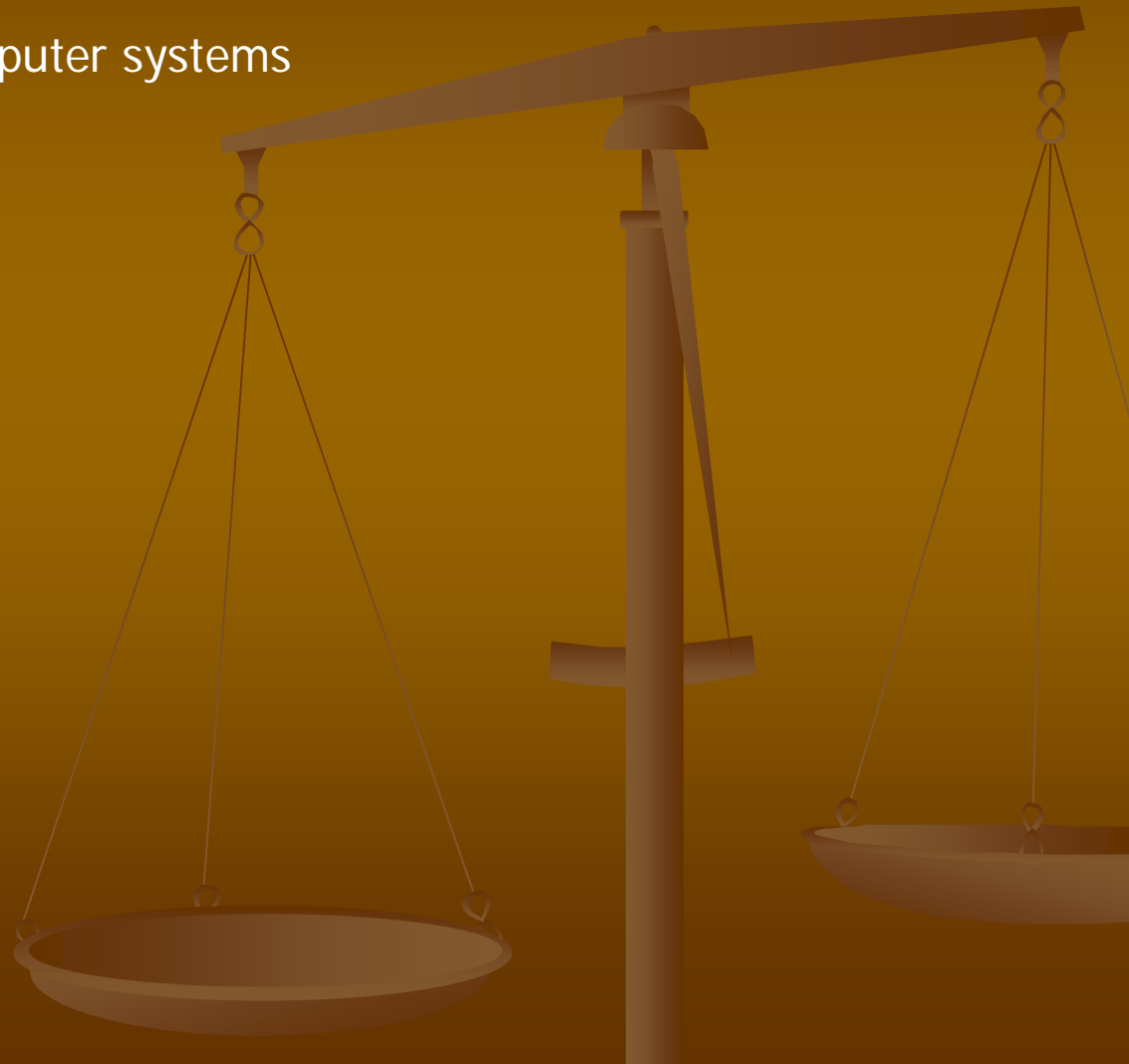
What most people think of computer systems

Rich sources of information

Large Drives

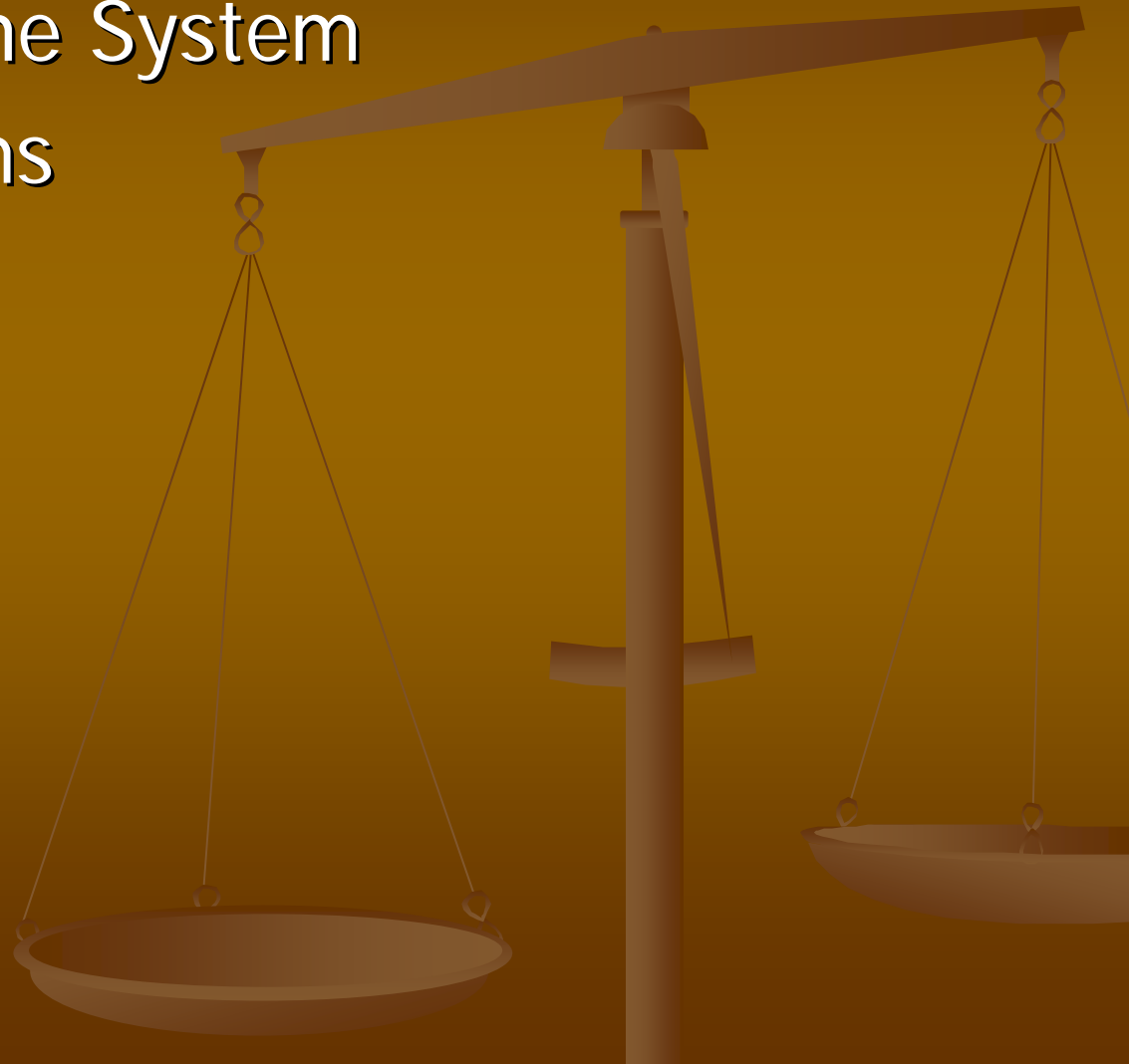
Portable Media

Optical Media



Communication Systems

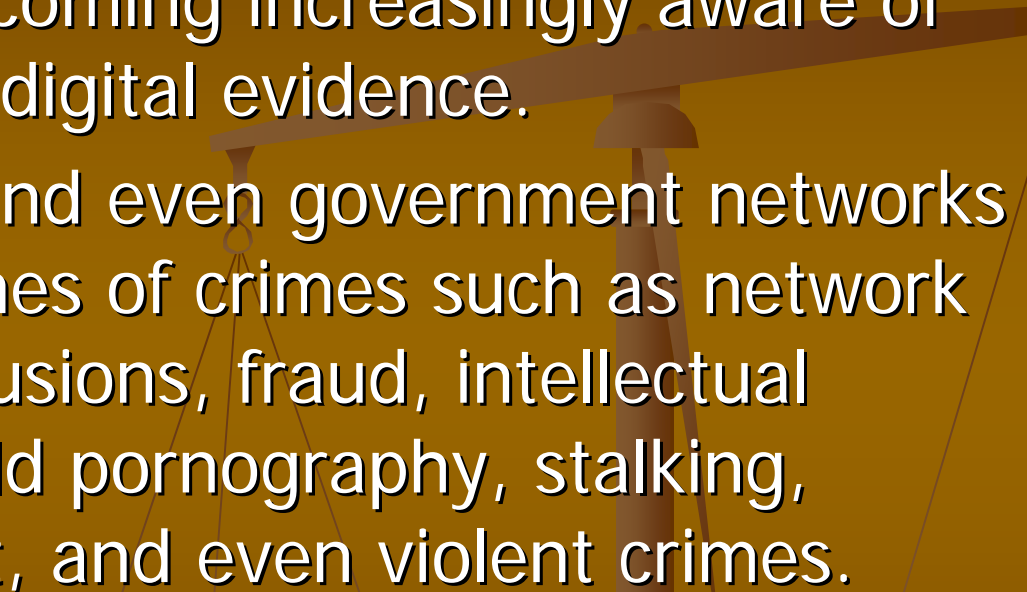
- Traditional Phone System
- Wireless Systems
- Internet



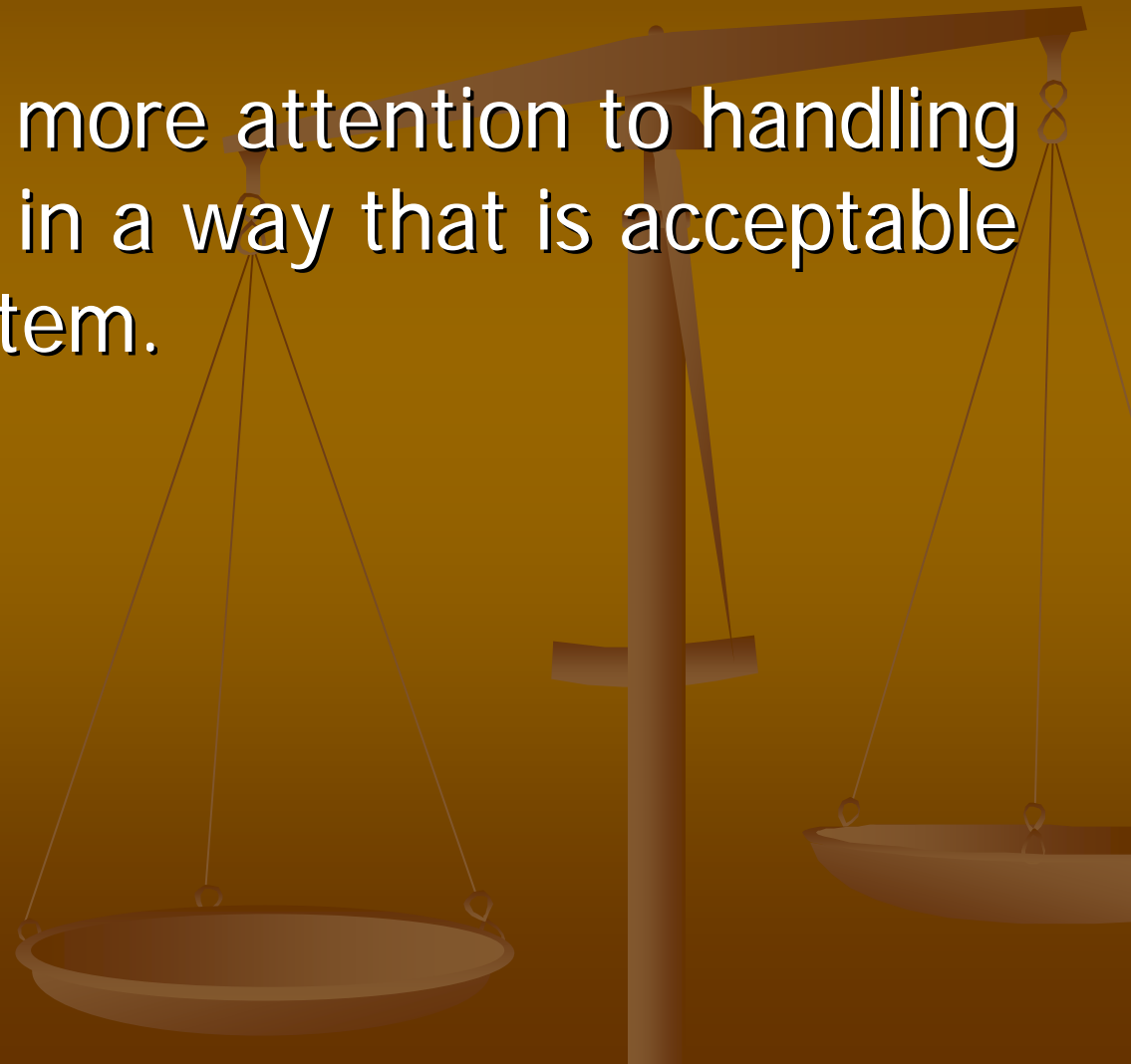
Embedded Computer Systems

- Satellite Phones
- Cell Phones
- PDA's
- Smart Cards
- GPS
- Microwaves

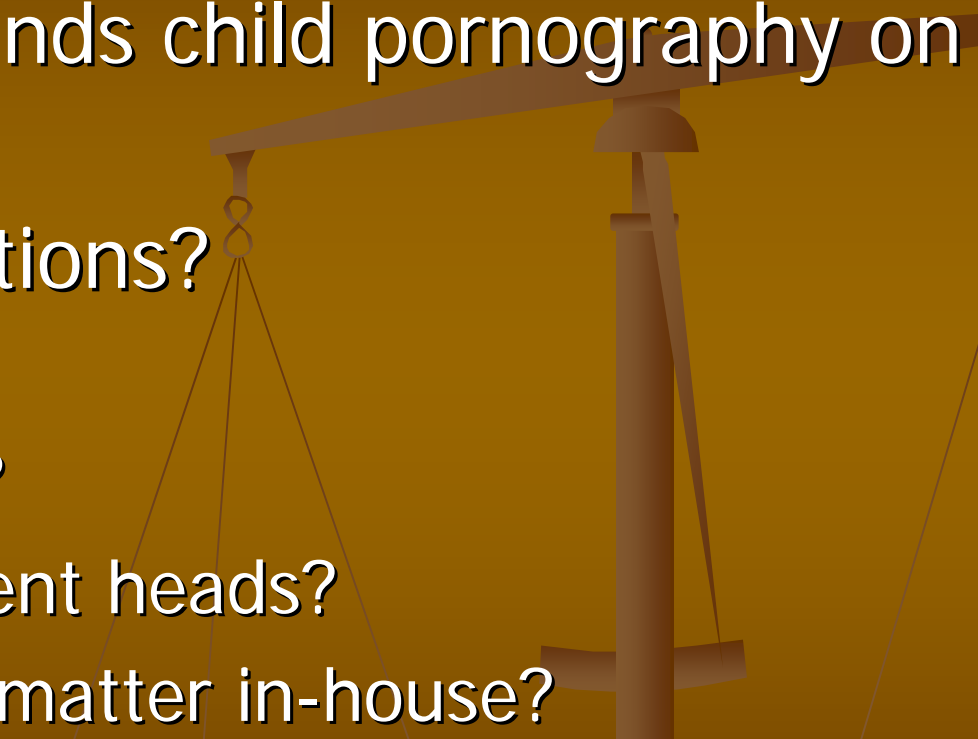


- 
- Attorneys, police, the military, and the private industry are all becoming increasingly aware of the importance of digital evidence.
 - Private company and even government networks are becoming scenes of crimes such as network and computer intrusions, fraud, intellectual property theft, child pornography, stalking, sexual harassment, and even violent crimes.

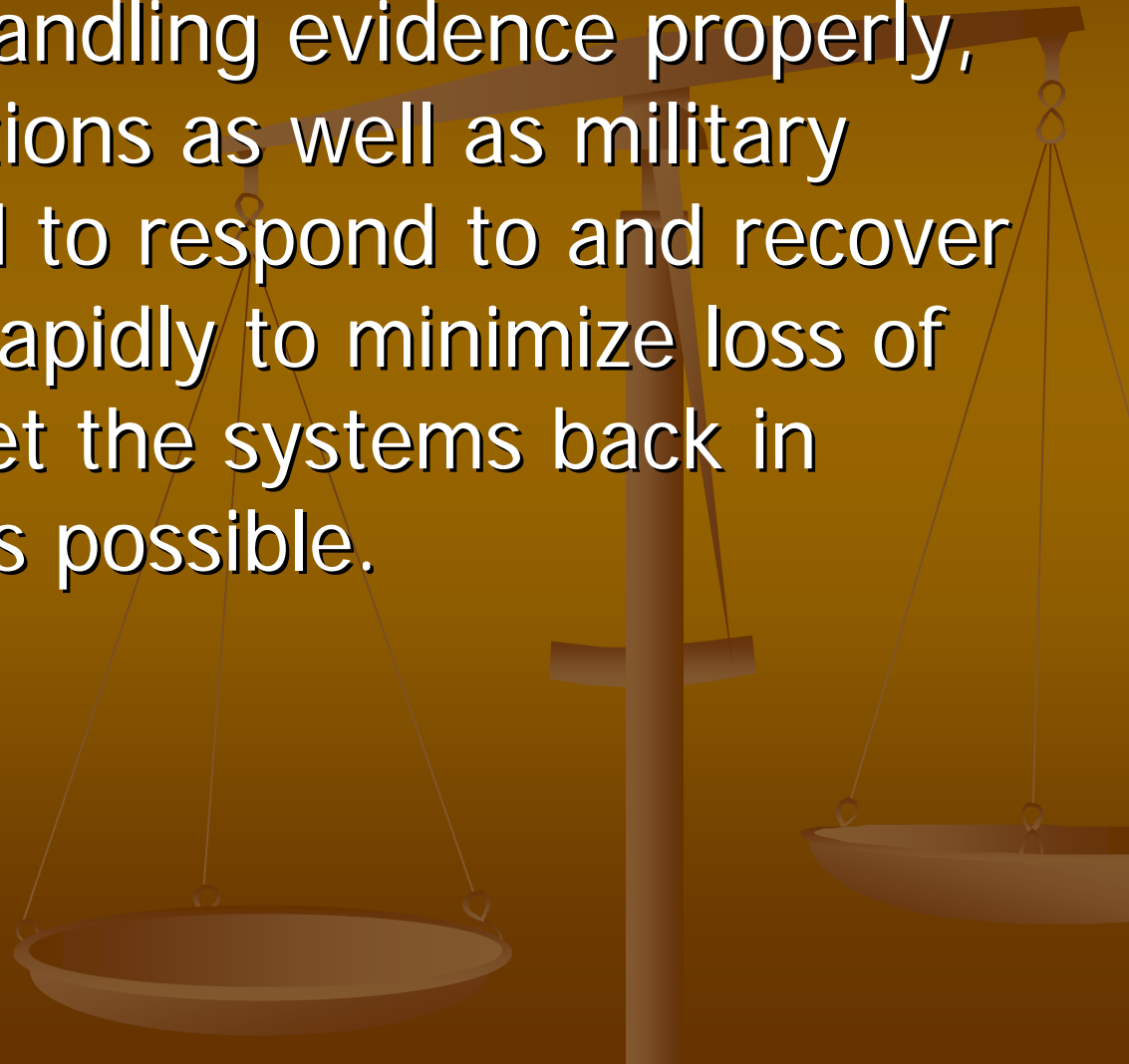
- More and more organizations are considering legal remedies when criminals target them.
- They are giving more attention to handling digital evidence in a way that is acceptable to the court system.



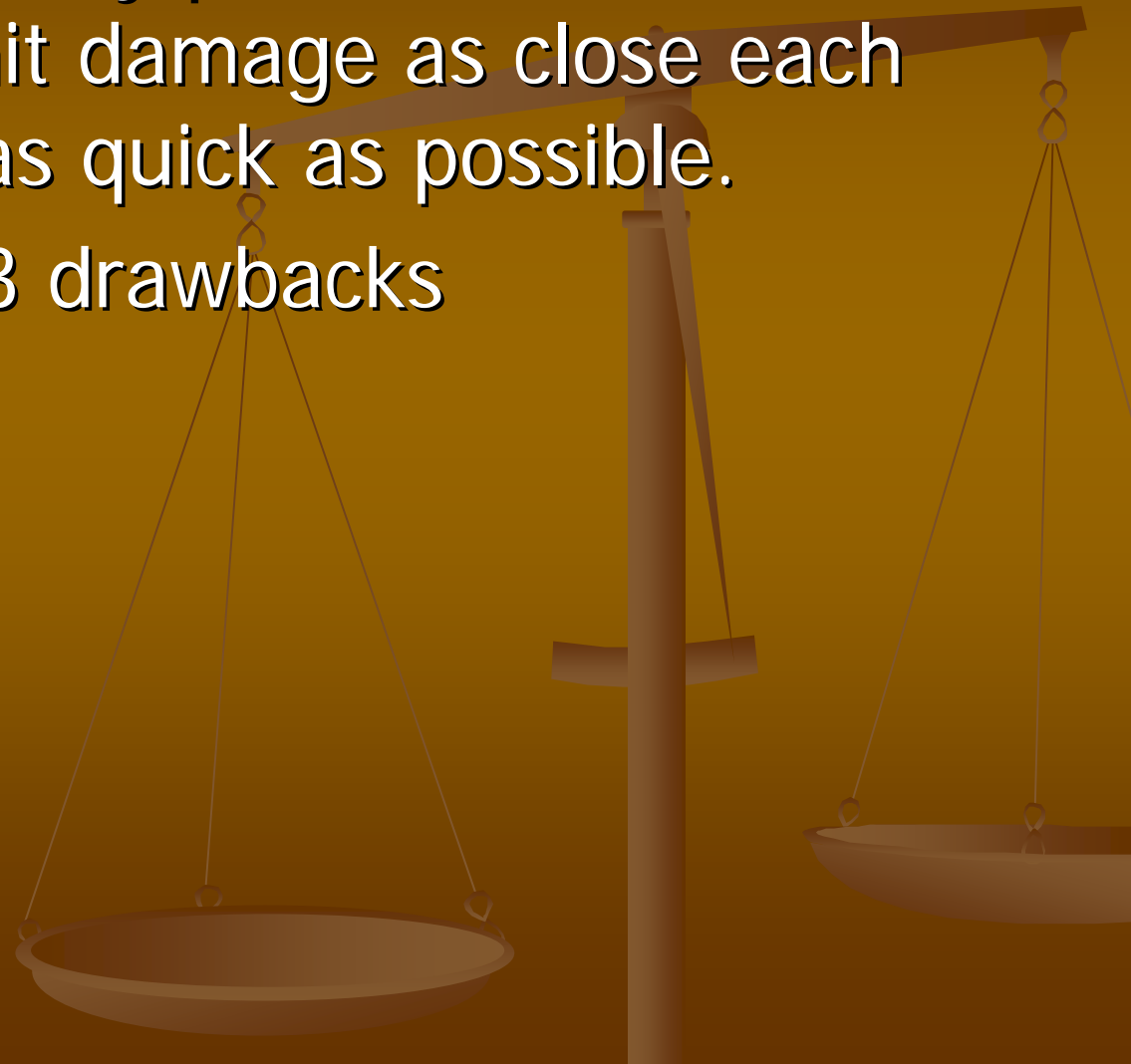
Discussion

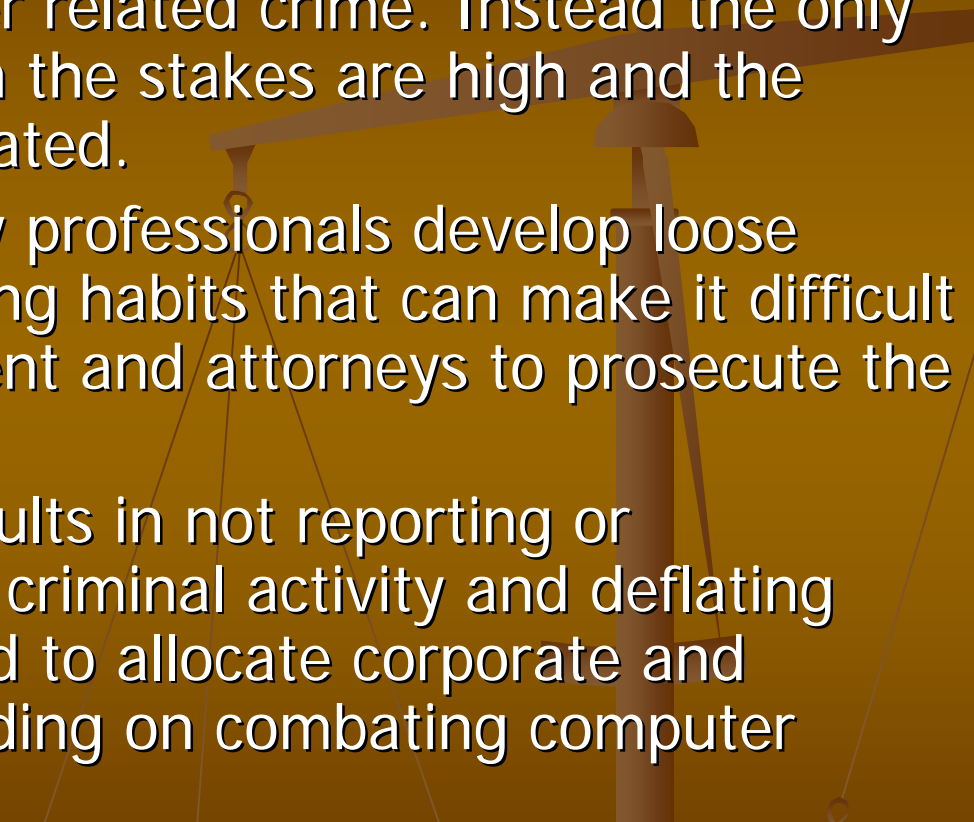
- System Admin finds child pornography on network
 - What are his options?
 - Delete?
 - Call Authorities?
 - Notify Department heads?
 - Investigate the matter in-house?
- 

- In addition to handling evidence properly, private corporations as well as military operations need to respond to and recover from incidents rapidly to minimize loss of evidence and get the systems back in order as soon as possible.

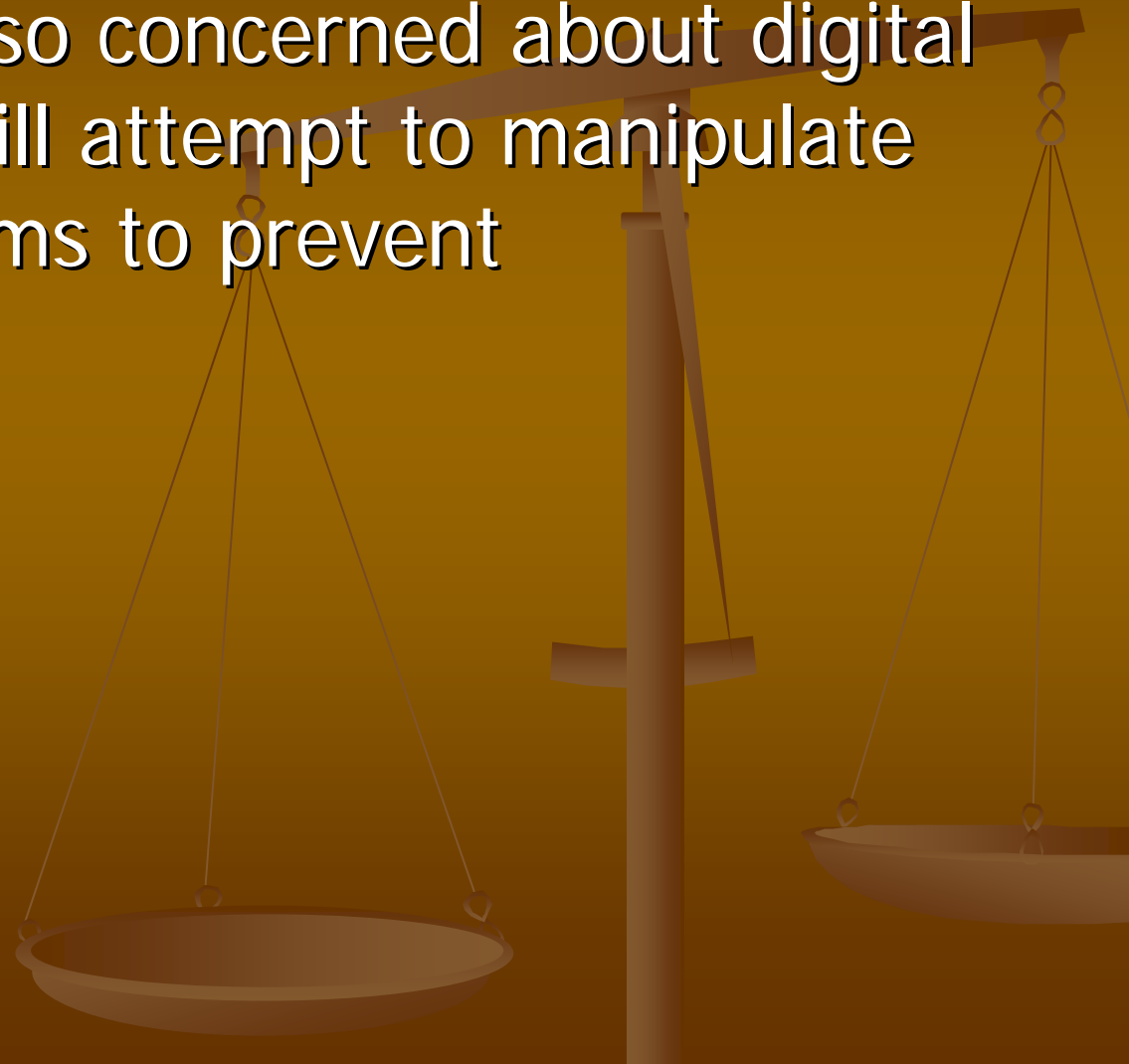


- Computer security professionals attempt to limit damage as close each investigation as quick as possible.
- This leads to 3 drawbacks



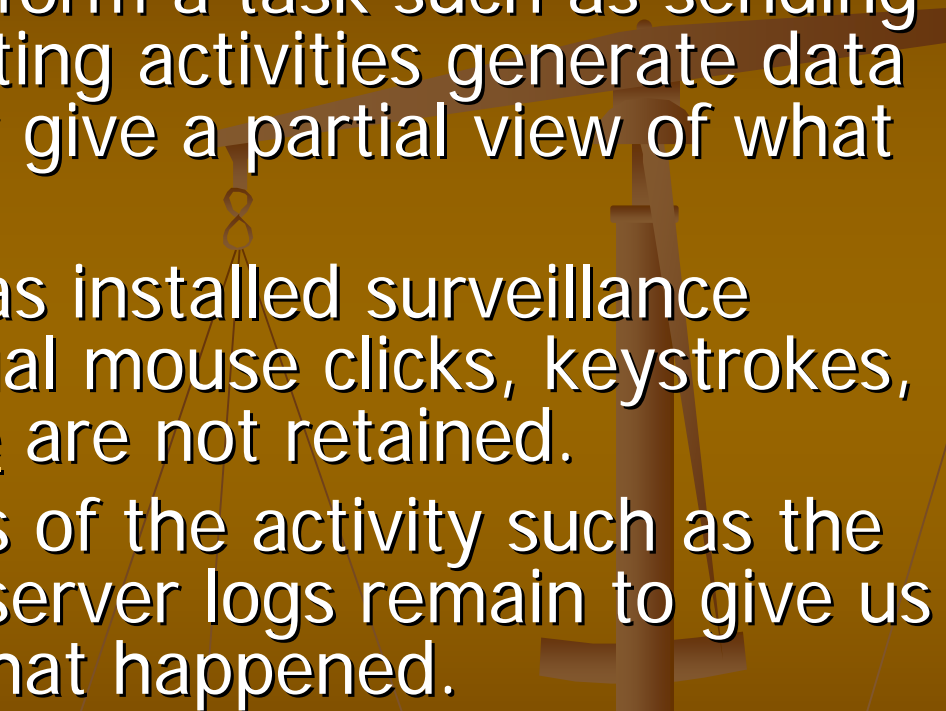
- 
- Each unreported incident robs attorneys and law enforcement an opportunity to learn about the basics of computer related crime. Instead the only get involved when the stakes are high and the cases are complicated.
 - Computer security professionals develop loose evidence processing habits that can make it difficult for law enforcement and attorneys to prosecute the offender.
 - This approach results in not reporting or underreporting of criminal activity and deflating stats that are used to allocate corporate and government spending on combating computer crime.

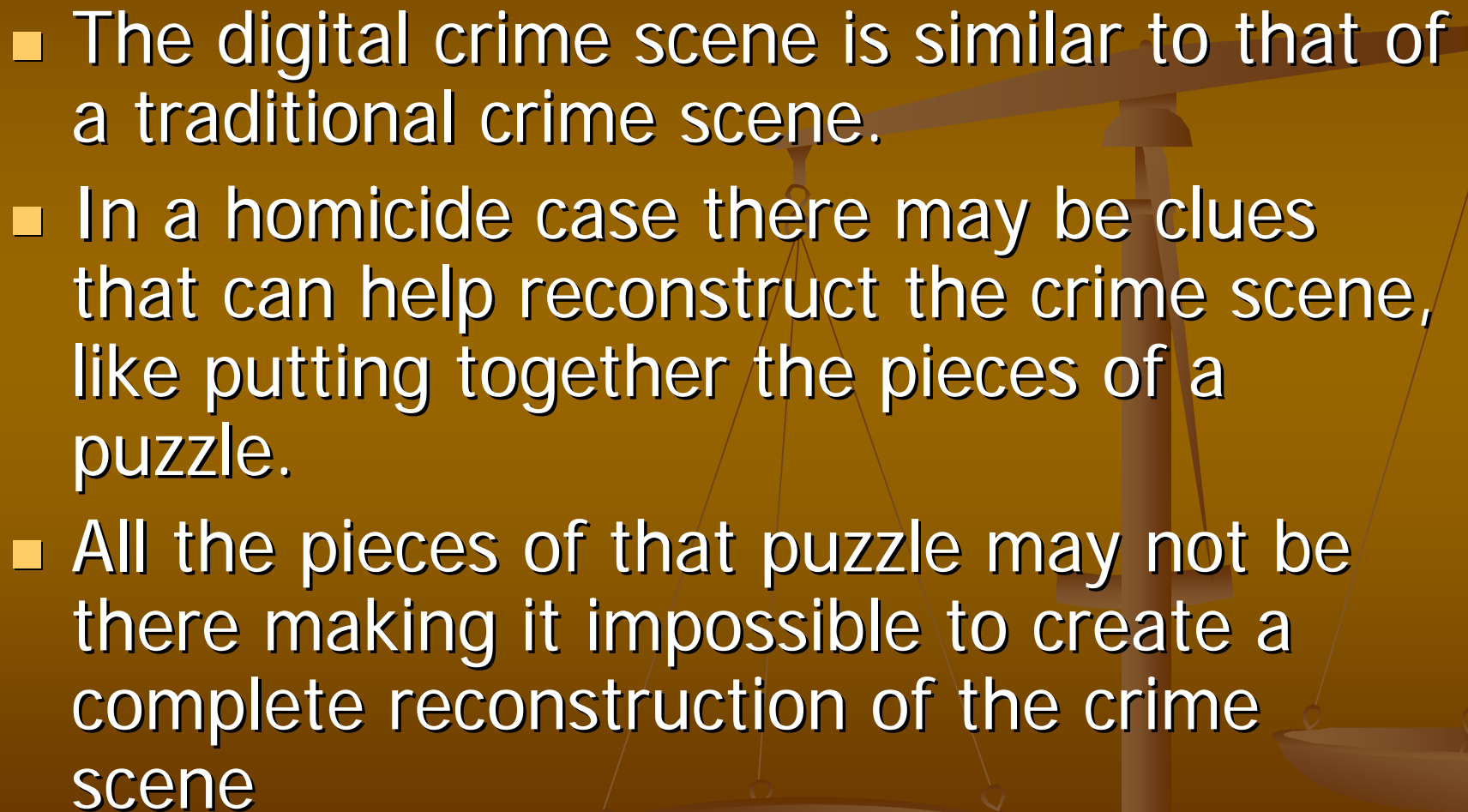
Criminals are also concerned about digital evidence and will attempt to manipulate computer systems to prevent apprehension.

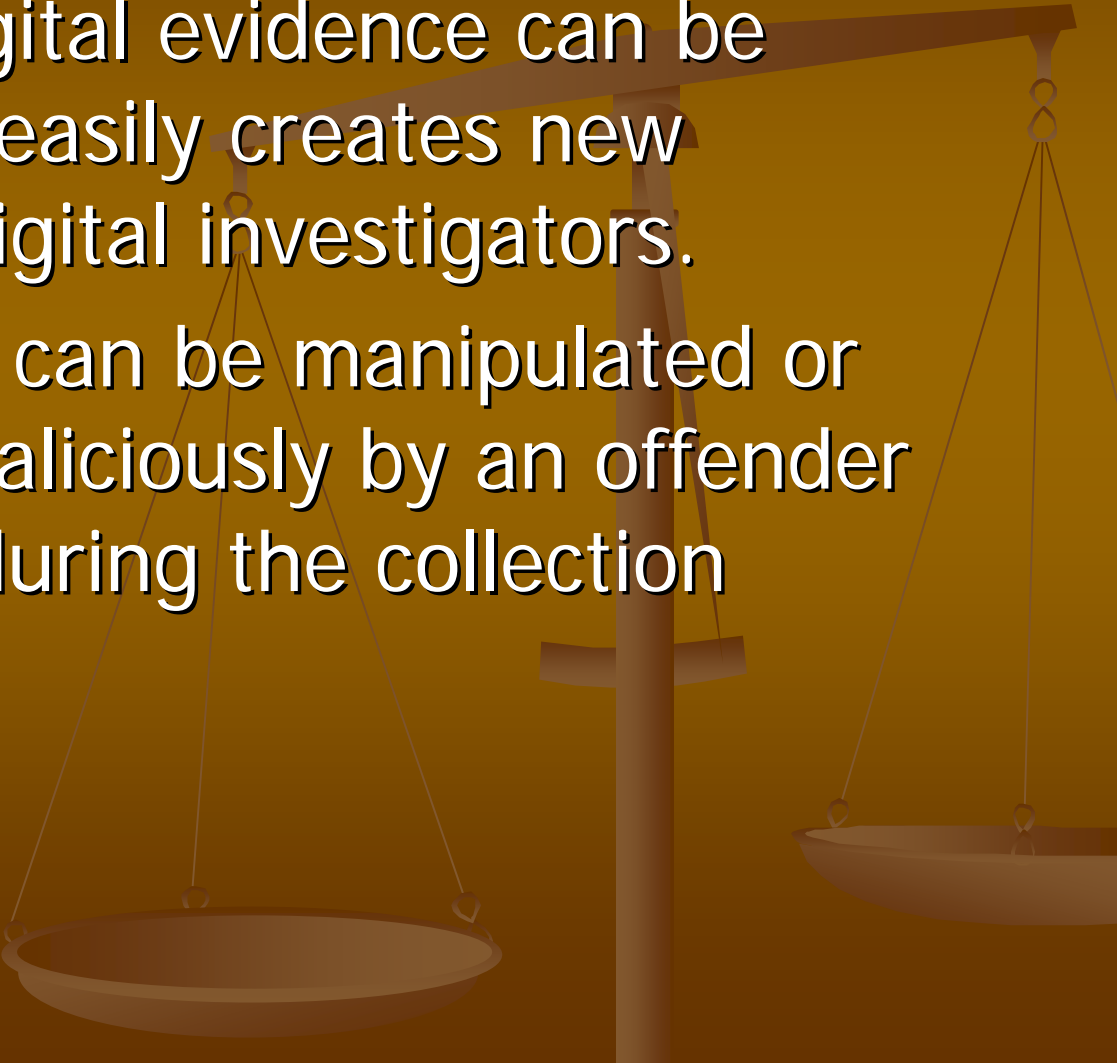


CHALLENGING ASPECTS OF DIGITAL EVIDENCE



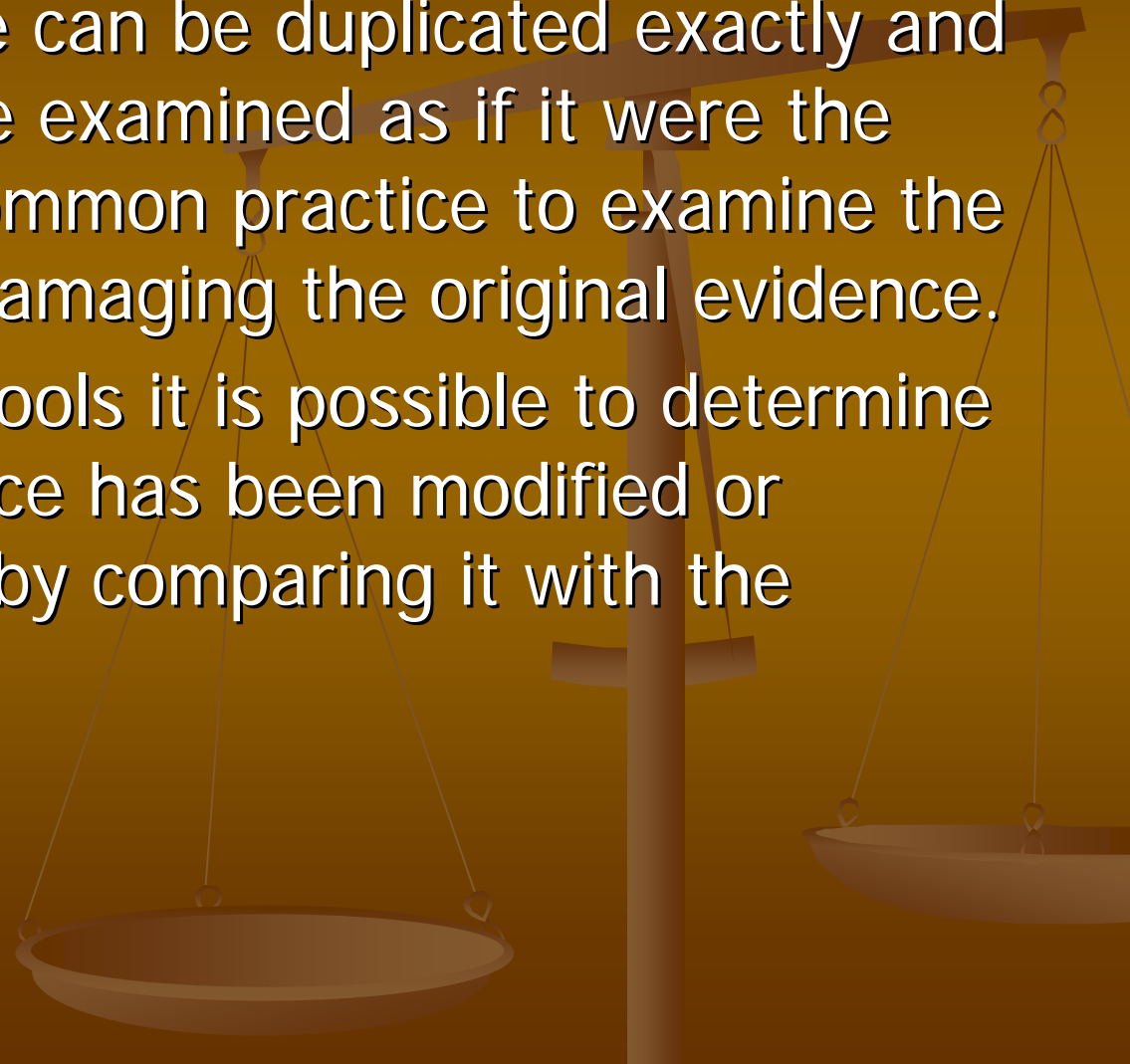
- 
- Digital evidence is generally an abstraction of some event or digital object. When a computer is instructed to perform a task such as sending an email, the resulting activities generate data remnants that only give a partial view of what occurred.
 - Unless someone has installed surveillance equipment individual mouse clicks, keystrokes, and other minutiae are not retained.
 - Only certain results of the activity such as the email message or server logs remain to give us a partial view of what happened.

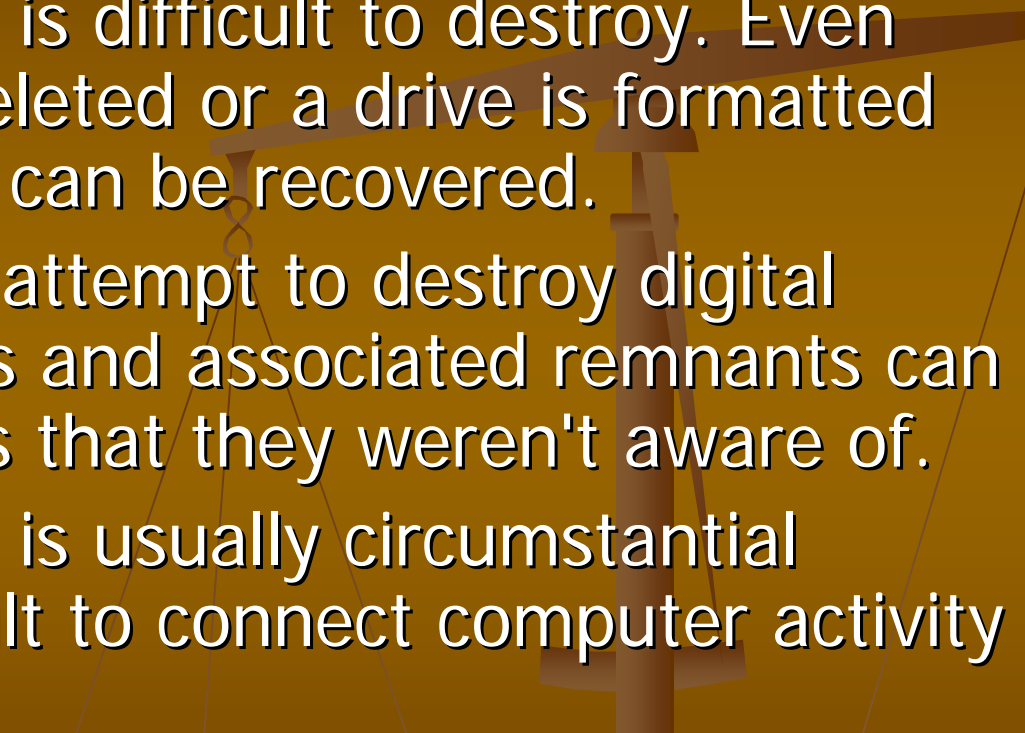
- 
- The digital crime scene is similar to that of a traditional crime scene.
 - In a homicide case there may be clues that can help reconstruct the crime scene, like putting together the pieces of a puzzle.
 - All the pieces of that puzzle may not be there making it impossible to create a complete reconstruction of the crime scene

- 
- The fact that digital evidence can be manipulated so easily creates new challenges for digital investigators.
 - Digital evidence can be manipulated or altered either maliciously by an offender or accidentally during the collection

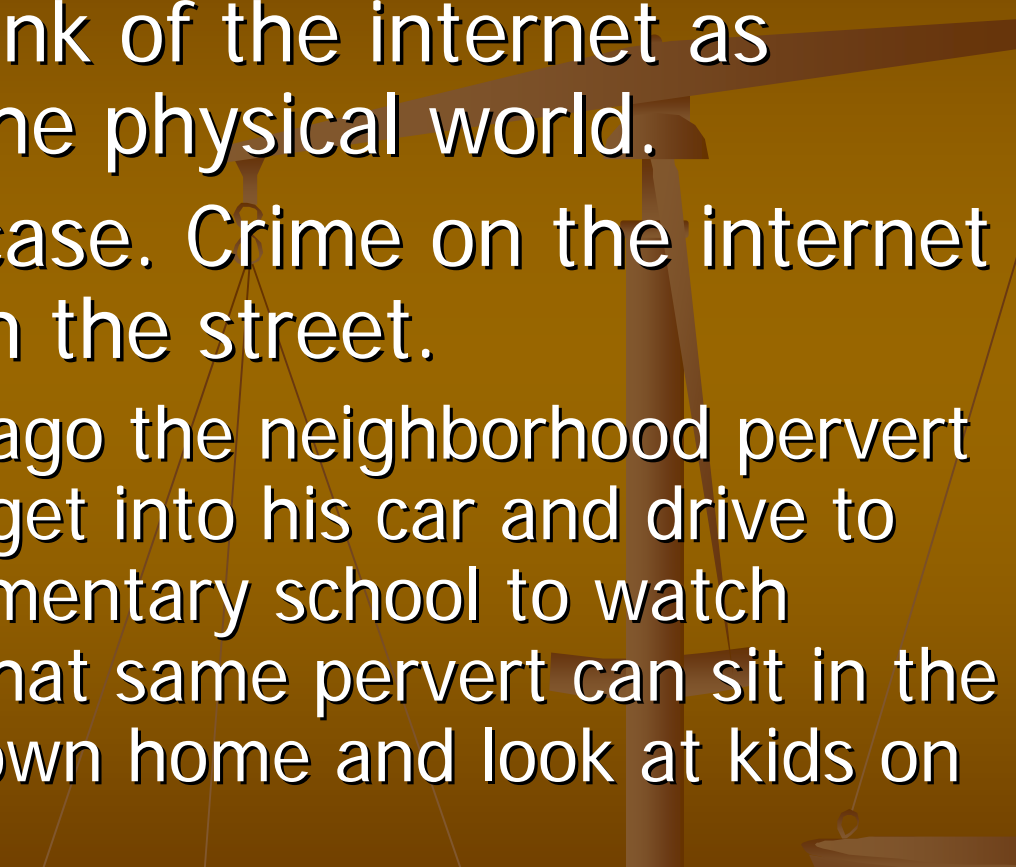
Digital evidence has several features that mitigate this problem.

- Digital evidence can be duplicated exactly and the copy can be examined as if it were the original. It is common practice to examine the copy to avoid damaging the original evidence.
- With the right tools it is possible to determine if digital evidence has been modified or tampered with by comparing it with the original.



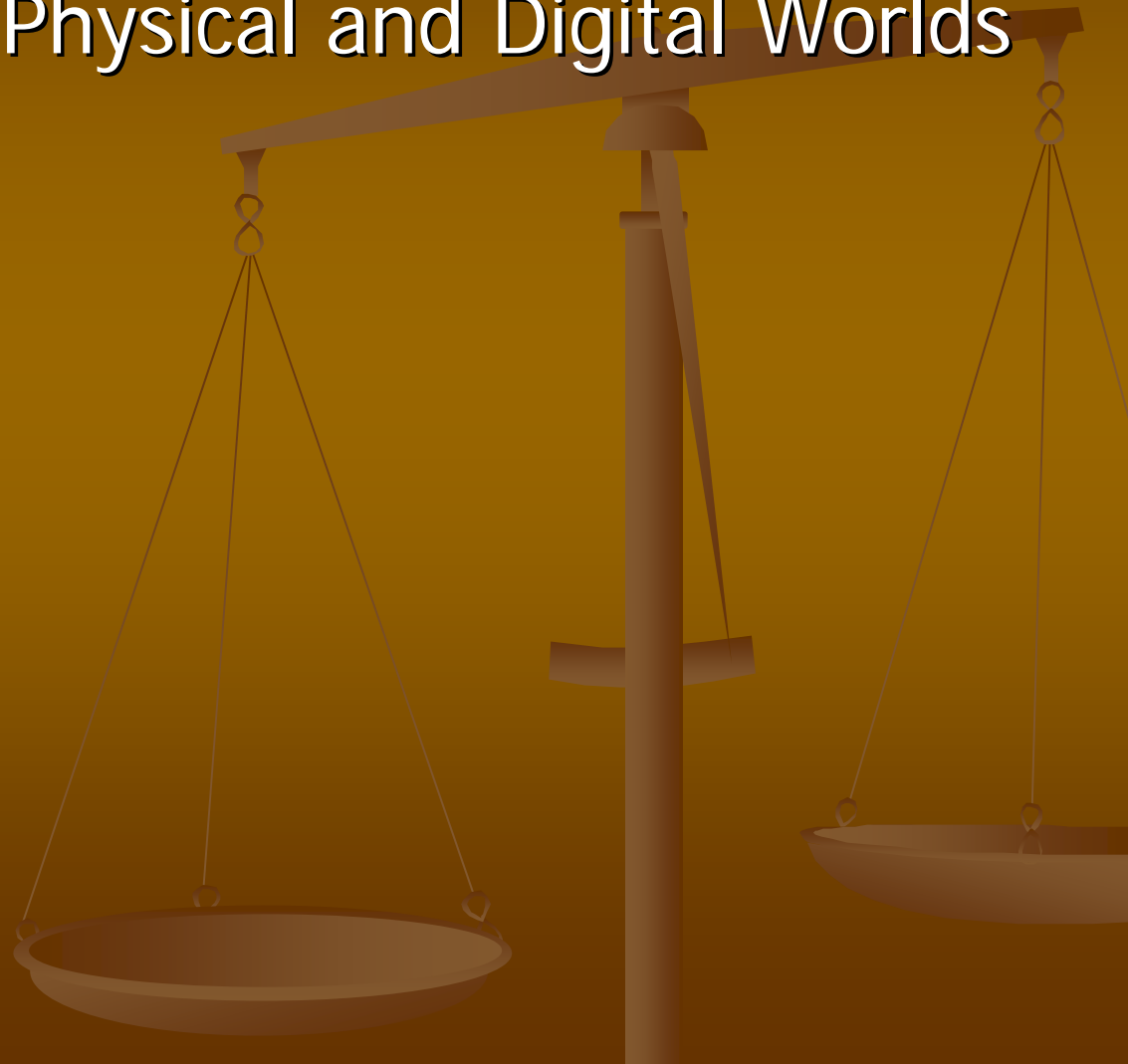
- 
- Digital evidence is difficult to destroy. Even when a file is deleted or a drive is formatted digital evidence can be recovered.
 - When criminals attempt to destroy digital evidence, copies and associated remnants can remain in places that they weren't aware of.
 - Digital evidence is usually circumstantial making it difficult to connect computer activity to an individual.

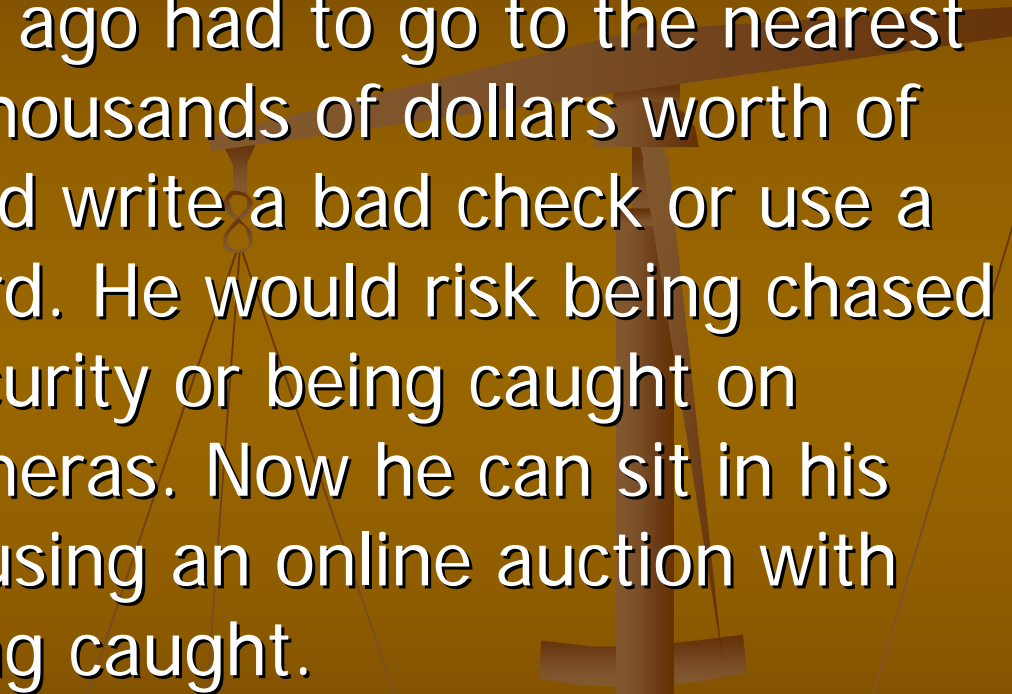
FOLLOWING THE CYBERTRAIL

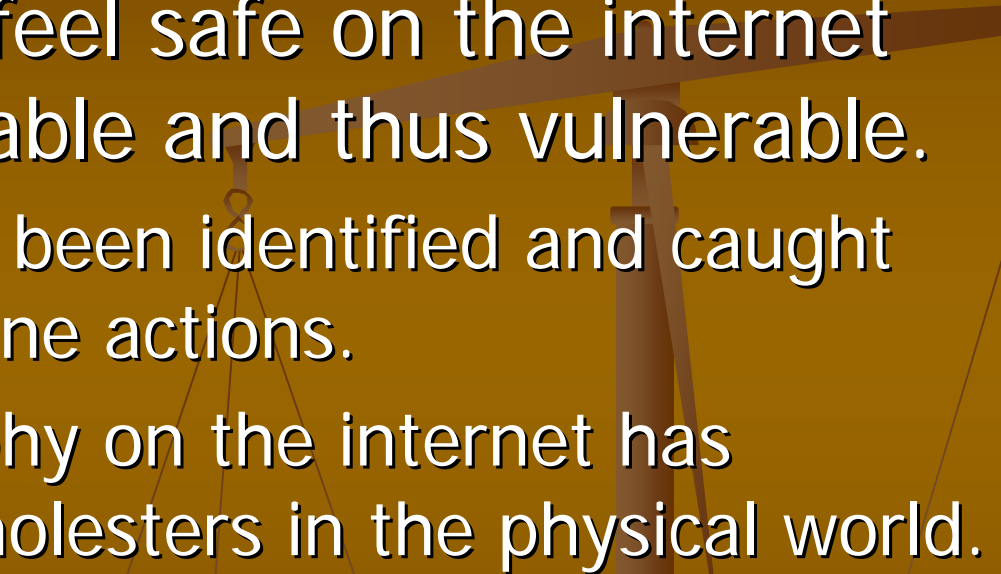
- Many people think of the internet as separate from the physical world.
 - This is not the case. Crime on the internet mirrors crime on the street.
 - 10 to 15 years ago the neighborhood pervert had to walk or get into his car and drive to the nearest elementary school to watch children. Now that same pervert can sit in the comfort of his own home and look at kids on the internet.
- 

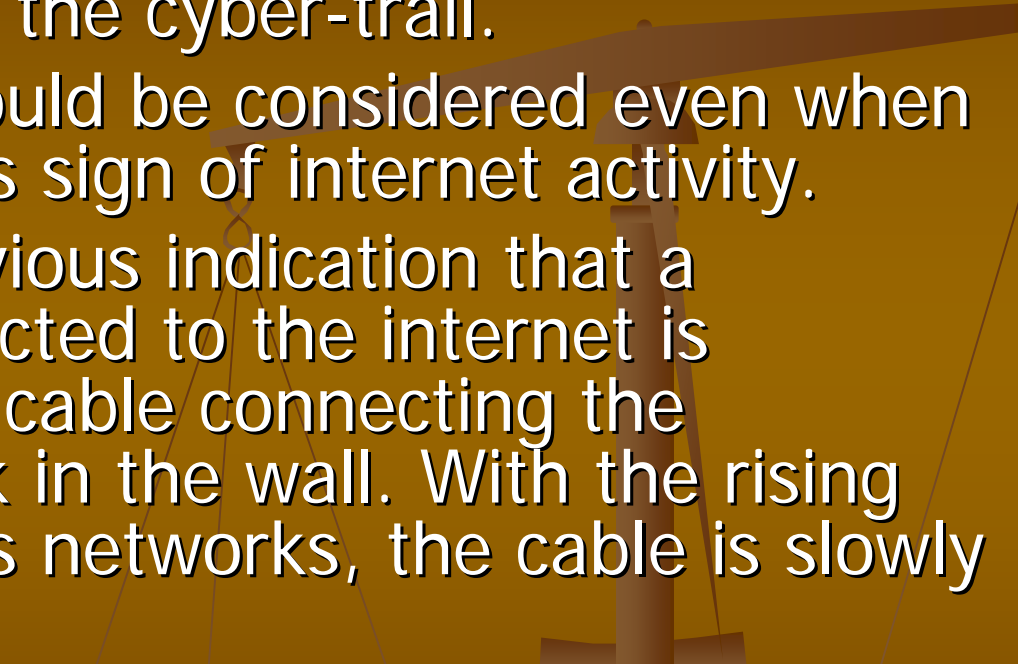
FOLLOWING THE CYBERTRAIL

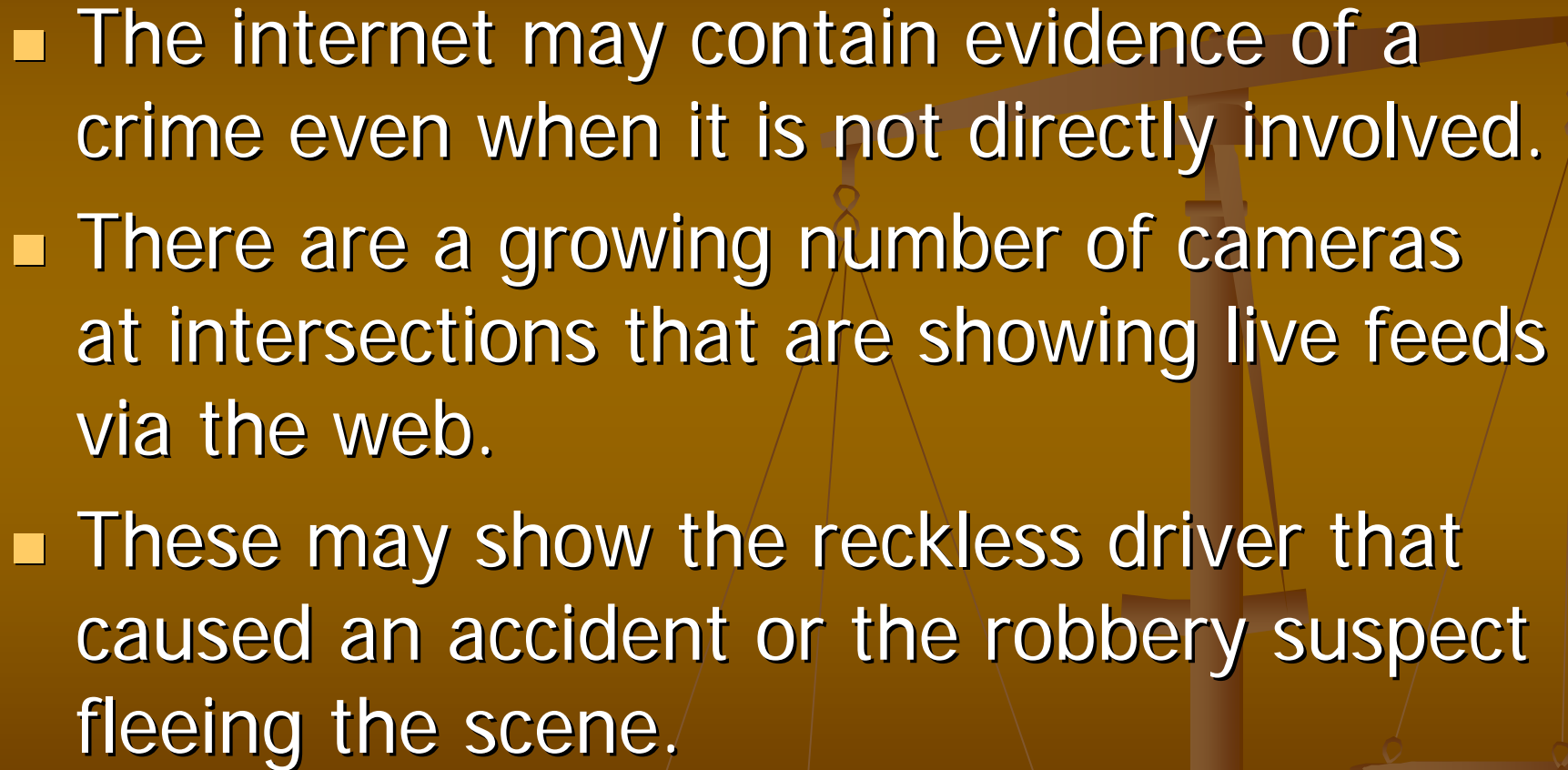
- Combination of Physical and Digital Worlds
- Auction Fraud

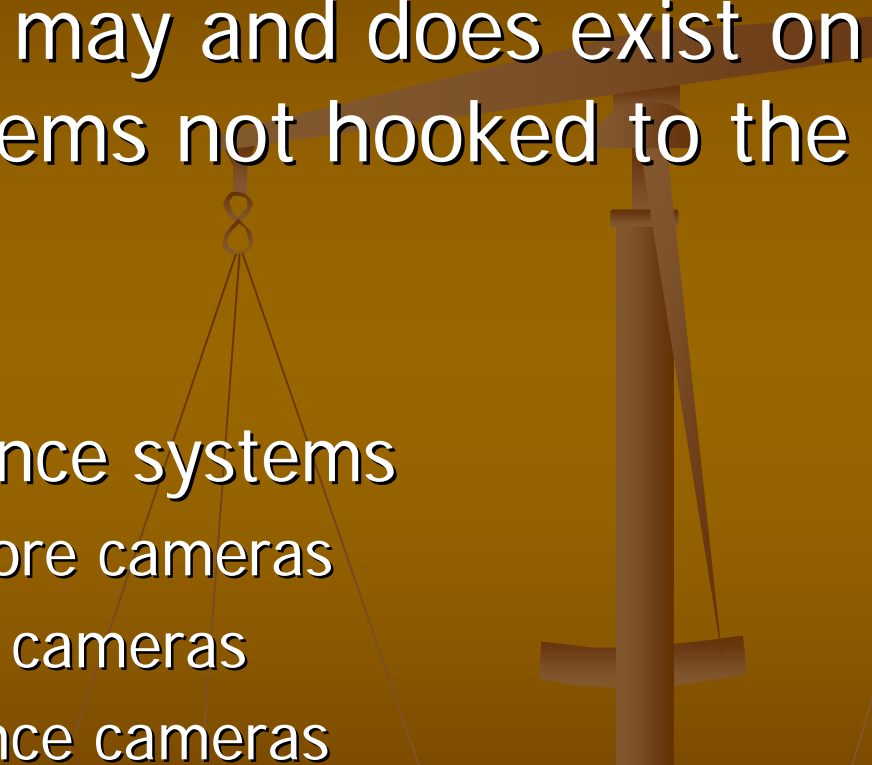


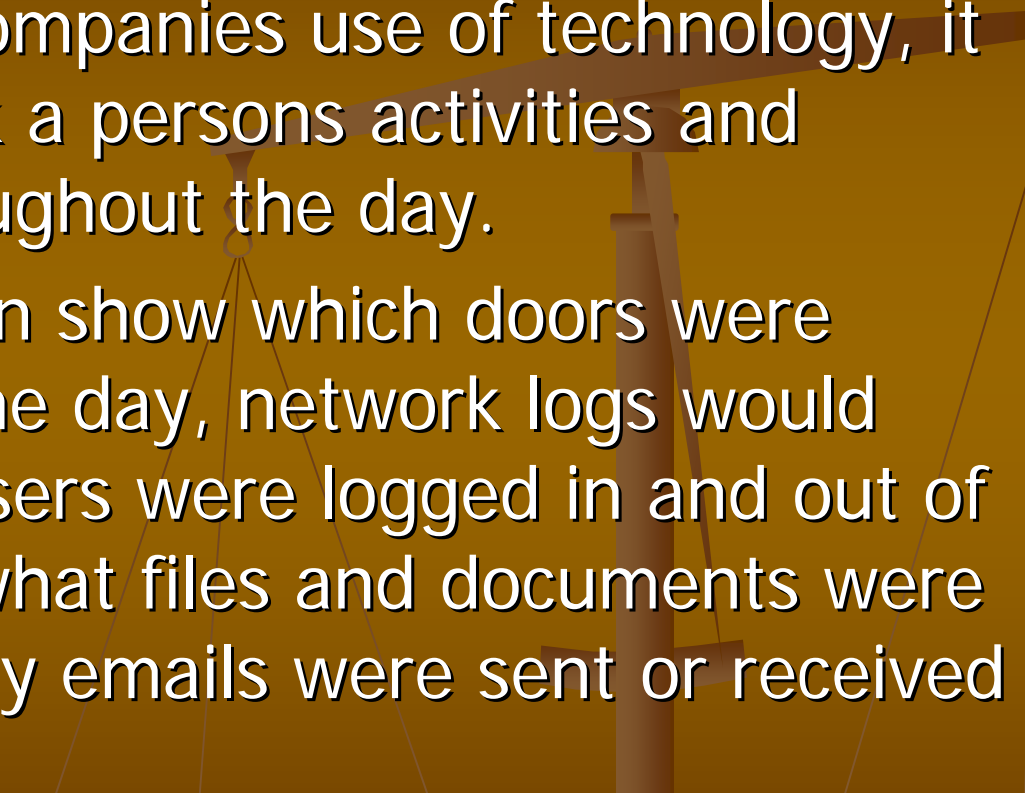
- 
- A thief 10 years ago had to go to the nearest store and buy thousands of dollars worth of merchandise and write a bad check or use a stolen credit card. He would risk being chased by the store security or being caught on surveillance cameras. Now he can sit in his home and buy using an online auction with little risk of being caught.

- 
- While criminals feel safe on the internet they are observable and thus vulnerable.
 - Murderers have been identified and caught due to their online actions.
 - Child pornography on the internet has exposed child molesters in the physical world.

- 
- The crimes of today and the future require us to become skilled at finding connections between crimes on the internet and crimes in the physical world by following the cyber-trail.
 - The cyber trail should be considered even when there is no obvious sign of internet activity.
 - Even the most obvious indication that a computer is connected to the internet is disappearing. The cable connecting the computer to a jack in the wall. With the rising number of wireless networks, the cable is slowly disappearing.

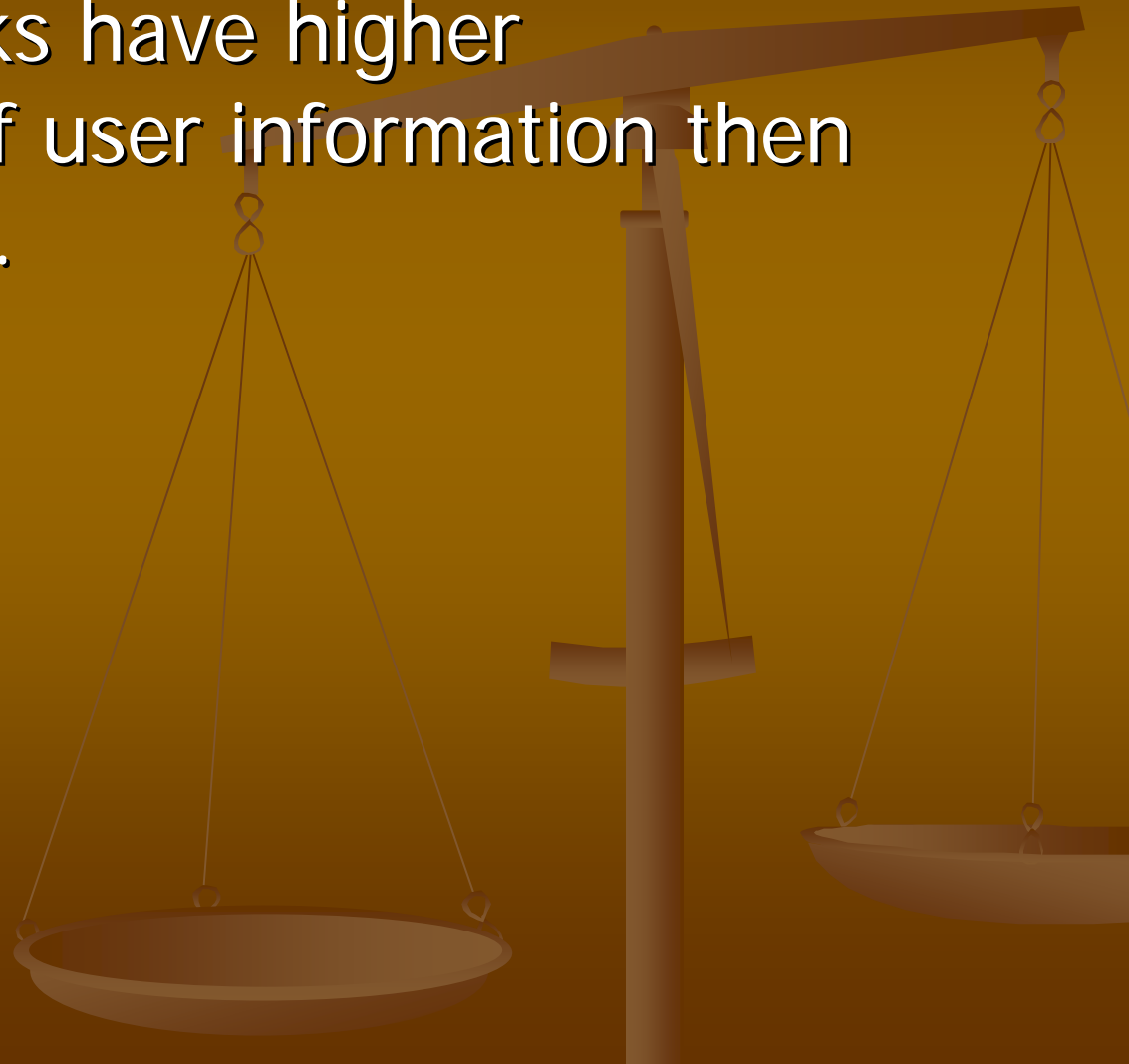
- 
- The internet may contain evidence of a crime even when it is not directly involved.
 - There are a growing number of cameras at intersections that are showing live feeds via the web.
 - These may show the reckless driver that caused an accident or the robbery suspect fleeing the scene.

- 
- Digital evidence may and does exist on commercial systems not hooked to the internet.
 - ATMs
 - Private surveillance systems
 - Convenience store cameras
 - Private security cameras
 - Home surveillance cameras

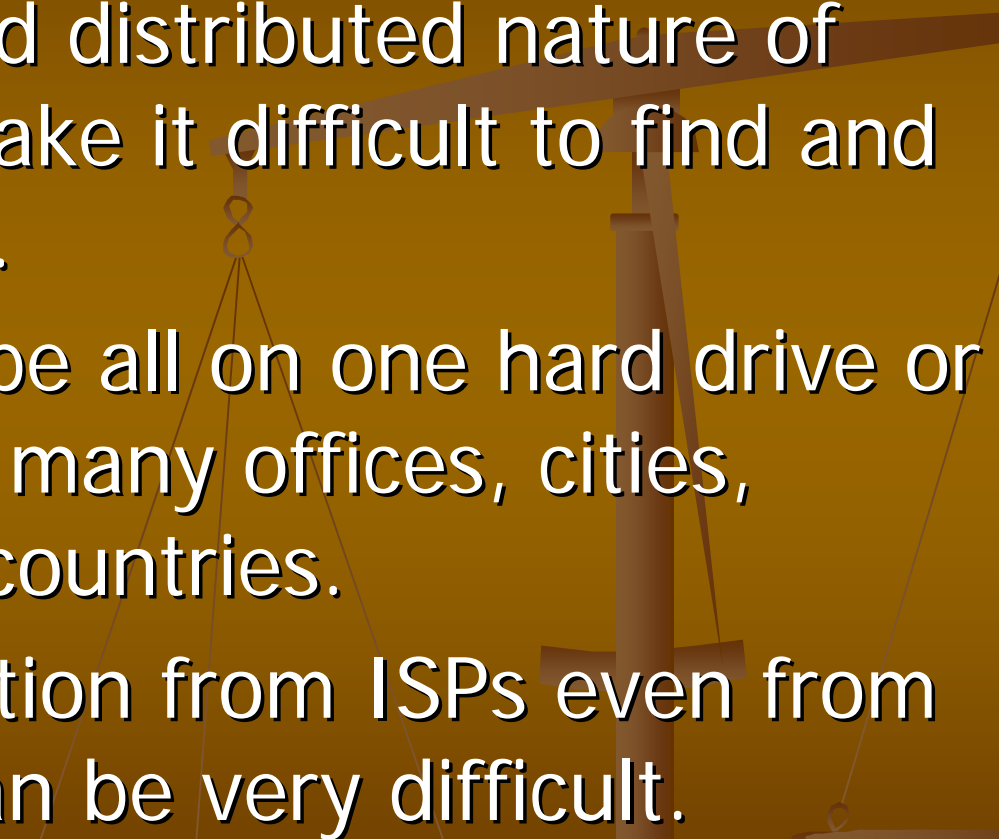
- 
- Depending on a companies use of technology, it is possible to track a persons activities and whereabouts throughout the day.
 - Proximity cards can show which doors were accessed during the day, network logs would show what time users were logged in and out of their computers, what files and documents were accessed and if any emails were sent or received and to whom.

Bits per square foot

- Smaller networks have higher concentration of user information than larger networks.

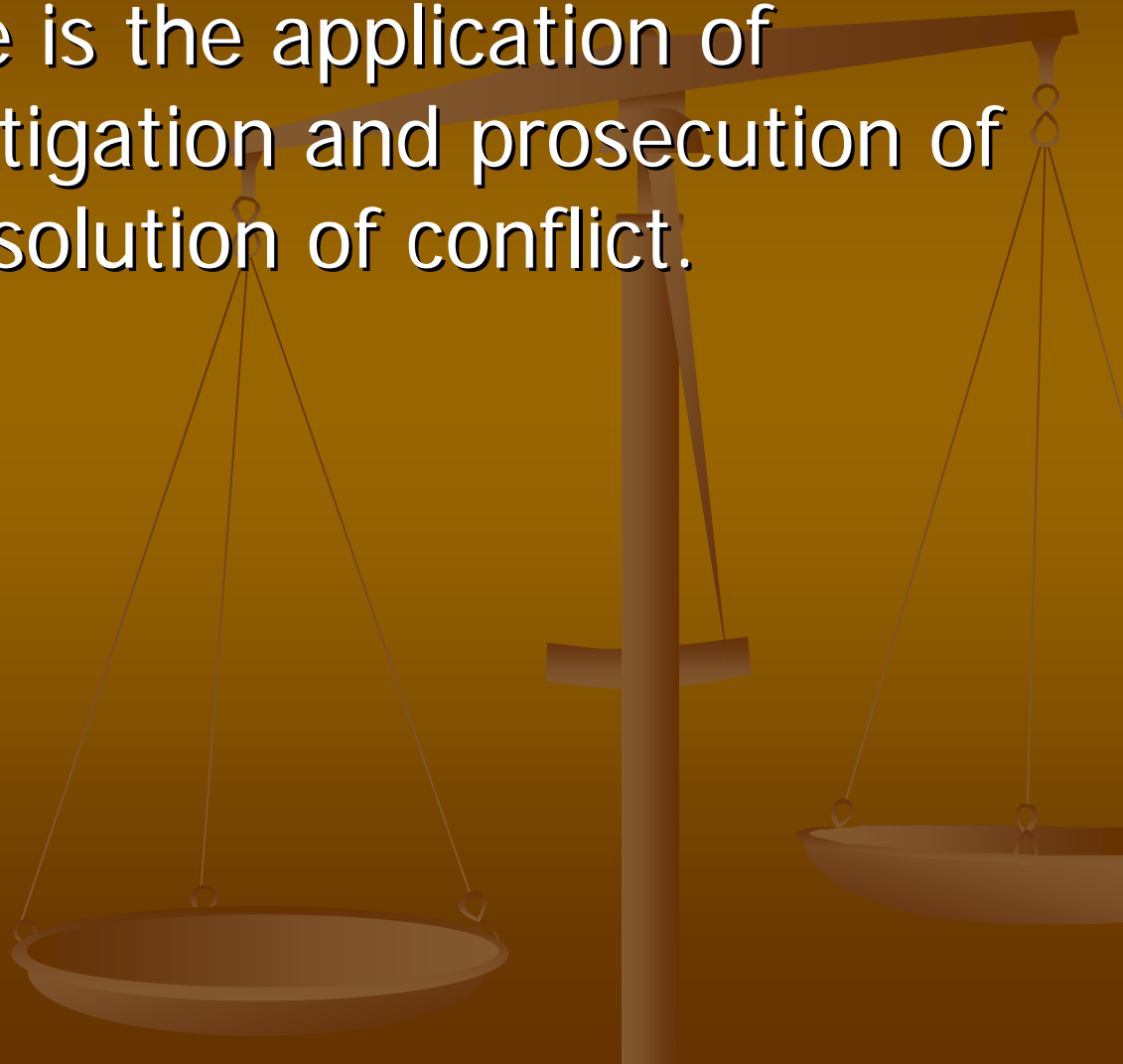


CHALLENGING ASPECTS OF THE CYBER-TRAIL

- The dynamic and distributed nature of networks can make it difficult to find and collect evidence.
 - Evidence could be all on one hard drive or distributed over many offices, cities, states, or even countries.
 - Getting cooperation from ISPs even from within the US can be very difficult.
- 

FORENSIC SCIENCE AND DIGITAL EVIDENCE

- Forensic science is the application of science to investigation and prosecution of crime, or the resolution of conflict.



Summary



- Digital Evidence abundant
- May be a source of evidence in any crime
- Investigator must be trained
- Educate the community
- Law Enforcement must work with Computer Security Professionals, Legal Professionals.
- All parties must be willing to ask for help from an "expert"
- Training for the Investigator must be constant

Contact

Bill Oettinger

Las Vegas Metropolitan Police
702-388-6571
woettinger@lvmpd.com

Digital Recovery Service

702-292-4645

william.oettinger@digital-recovery-service.com

