PUTTING THE SUSPECT AT THE COMPUTER

Michelle Kane, Trial Attorney

Computer Crime and Intellectual Property Section

Criminal Division, United States Department of Justice

OVERVIEW

Proving that the Defendant Committed the Crime

The Role of Circumstantial Evidence

Strategies for Collecting and Using Circumstantial Evidence in Cybercrime Cases

Conclusions

OVERVIEW

Proving that the Defendant Committed the Crime

The Role of Circumstantial Evidence

Strategies for Collecting and Using Circumstantial Evidence in Cybercrime Cases

Conclusions

- One of the biggest challenges of most computer crime cases is proving *who* was at the computer

- This proof will almost always depend on some type of *circumstantial evidence*

Scenarios

Fraudulent bank transfer using suspect’s account, traced to IP address assigned to suspect’s computer

Unauthorized access to restricted database from suspect’s government computer terminal

Threats made through email account registered in suspect’s name

How do you prove the suspect did it?

OVERVIEW

Proving that the Defendant Committed the Crime

The Role of Circumstantial Evidence

Strategies for Collecting and Using Circumstantial Evidence in Cybercrime Cases

Conclusions

Circumstantial Evidence

Definition: evidence based on *inference*

- **National legal systems may treat it differently, but it is generally distinguished from “direct evidence”**

- **The assertion of a “collateral fact” that allows a key fact in the case to be inferred**

Inference that *the suspect committed the crime*

Circumstantial Evidence

Electronic evidence may lead to a computer, but not to an *individual*

Absent direct evidence linking the individual to the crime, look for circumstantial evidence of:

- Access
- Knowledge
- Opportunity
- Motive
- State of mind

OVERVIEW

Proving that the Defendant Committed the Crime

The Role of Circumstantial Evidence

Strategies for Collecting and Using Circumstantial Evidence in Cybercrime Cases

Conclusions

Access

Suspect's *access* to computer resources used to commit the crime

- **Computer (hardware, software, files)**
- **Telephone or cable lines used for online access**
- **Online accounts (Email, online banking, social networking)**

May need to rule out others with access

Knowledge

Suspect's *knowledge* of information related to the crime

- Experience with the program, system or network that was used or compromised
- Computer training, education, experience or ability
- Familiarity with specific facts linked to crime
- Possession of passwords

Opportunity

Opportunity **for the suspect to commit the crime**

- **Use of a computer at the time of the criminal activity**
- **No credible alibi**

Motive

Motive **for the suspect to commit the crime**

- **Revenge**
- **Money (including blackmail, extortion)**
- **Politics**
- **Personal challenge**

State of Mind

The suspect’s *culpable state of mind*

- Deception
- Concealment
- Destruction of evidence

Don’t Forget Traditional Tools

The best circumstantial evidence may come from old-fashioned detective work, such as:

- Suspect and witness interviews
- Physical evidence
- Surveillance

Traditional evidence can corroborate electronic evidence

OVERVIEW

Proving that the Defendant Committed the Crime

The Role of Circumstantial Evidence

Strategies for Collecting and Using Circumstantial Evidence in Cybercrime Cases

Conclusions

Conclusions

Circumstantial evidence provides the key link between the suspect and the computer

Traditional circumstantial evidence complements electronic evidence in making a stronger case that the suspect was responsible

How do you counter defense tactics?

OVERVIEW

Common Cyber Crime Defenses

Defense Tactics and Ways to Counter Them

Conclusions

OVERVIEW

Common Cyber Crime Defenses

Defense Tactics and Ways to Counter Them

Conclusions

Universal Principles

Defendants all over the world use similar approaches in cybercrime cases

- Confuse everything
- Imply guilt or bad motives for all witnesses (except defendant)
- Cast the technology and evidence as incomprehensible

Common Cyber Crime Defense Tactics

Using technology to create confusion

Pointing to absence of direct evidence

Claiming to lack technical ability

Suggesting someone else controlled the computer

Implying that evidence was planted by the authorities

OVERVIEW

Common Cyber Crime Defenses

Defense Tactics and Ways to Counter Them

Conclusions

Using Technology to Create Confusion

Defense will:

- Make the technology seem more complicated than it really is
- Exploit general fear of technology and computers
- Create doubt in the mind of the factfinder
- “If I can’t understand the facts, how can I be sure the defendant did it?”

Using Technology to Create Confusion: Response

Simplify everything

Introduce and explain the technology early

Know your audience

Prepare witnesses to explain the technology using clear language

Use visual aids and exhibits

Using Technology to Create Confusion: Response

Do not forget to present non-electronic evidence

- Fact witnesses
- Surveillance records
- Physical evidence
- Motive
- Suspicious behavior

Corroborates electronic evidence

Pointing to Absence of Direct or Physical Evidence

Defense will:

- Argue that your case depends on “circumstantial evidence
- Point to a lack of physical evidence like DNA or fingerprints
- Suggest that this makes your case weaker than one based on “direct” evidence

Pointing to Absence of Direct or Physical Evidence: Response

Argue (if possible) that circumstantial evidence is as compelling as direct evidence

Explain that lack of “direct” evidence is typical of computer crime cases

Emphasize the lack of any viable alternative suspect

Claiming to Lack Technical Ability

Defense will:

- Claim that the crime required someone with special computer expertise
- Suggest that defendant does not have special skills or is not smart enough to have carried out the criminal acts

This is often combined with the first tactic -- sowing confusion through technology

“Playing Dumb”

Claiming to Lack Technical Ability: Response

Research your defendant's technical background

Equipment and software can demonstrate sophistication

Examine Internet history for a record of self-education

Interview suspect and associates regarding computer knowledge

Suggesting Someone Else Was in Control

Defense will:

- Argue that the computer or service was hijacked by an unknown agent
- "A virus took over the computer and downloaded material from the Internet"
- "The email was spoofed"

This is often combined with the first tactic -- sowing confusion through technology

Suggesting Someone Else Was in Control: Response

Show how access to the suspect's computer was limited

Demonstrate that others with access to the computer did not commit the crime

Explain (through forensic examiner) how we know that no program or outside person controlled the computer

Implying that Evidence Was Planted

Defense will:

- Attack the collection of electronic evidence, chain of custody, and forensic examination

- Try to impeach the forensic examiner and everyone who touched the evidence

Implying that Evidence Was Planted: Response

Prove secure chain of custody for the digital media

Introduce records showing when the suspect's files were created, accessed, or modified

Describe in court the devices used to image and record the evidence

Explain safeguards of the forensic process

CONCLUSIONS

The same technology and electronic evidence can be used by the defense to confuse and by the prosecution to enlighten

Prosecutors, police and forensic investigators working together can effectively anticipate, prepare for, and counter common cybercrime defenses

Questions

?

WWW.CYBERCRIME.GOV

Computer Crime and Intellectual Property Section (CCIPS)
of the Criminal Division of the U.S. Department of Justice