NIJ Electronic Crime Technology Center of Excellence

Robert J. O'Leary, CFCE; DFCP
Director
NIJ Electronic Crime Technology Center of Excellence
550 Marshall St. Suite B
Phillipsburg, NJ 08865

NIJ Electronic Crime Technology Center of Excellence

NIJ ECTCoE

The Criminal Justice Electronic Crime Technology Center of Excellence provides scientific and technical support to NIJ's research and development efforts; supports the demonstration, transfer, and adoption of appropriate technology into practice by law enforcement and corrections agencies, courts, and public crime laboratories; assists in the development and dissemination of technology guidelines and standards; and provides technology assistance, information, and support to law enforcement and other criminal justice agencies. .

ECTCoE's Strategic Goals align with NIJ's goals

NIJ strategic goals

- **Increase the Nation's capacity to prevent and control crime**
- **Improve the fair administration of justice**
- **Reduce the impact of crime on victims and hold offenders accountable**
- **Increase understanding of justice issues and develop successful interventions**

Electronic Crime Goals and Objectives

NIJ ECTCOE Electronic Crime Technology Center of Excellence

- **Goal:**
  - To assist state and local law enforcement agencies to effectively and efficiently investigate, analyze, preserve, and present digitally stored information of evidentiary value
- **Objectives:**
  - RESEARCH AND DEVELOPMENT of emerging technologies required for Electronic Crime Investigations and Digital Evidence Recovery as recommended or directed by the E-Crime TWG, federal partners, or Congress
  - TEST AND EVALUATE technology to provide unbiased information to the federal, State, local, and tribal law enforcement communities
  - DEMONSTRATION of cutting edge technologies in an operational environment to the law enforcement community
  - STANDARDS that improve technology reliability, accuracy, and admissibility
  - OUTREACH to provide unbiased information to the state and local law enforcement community on electronic crime and digital evidence recovery technology related issues

Objectives

- **Support the Electronic Crime TWG**
- **Tool Testing & Evaluation**
  - Test electronic crime & digital evidence tools & technologies
- **Requirements**
  - Identify operational requirements
- **Technology**
  - Deliver technology demonstrations/evaluations of emerging technologies
- **Standards**
  - Support professional, laboratory and technology standards
- **Coordination**
  - Support coordinated efforts among law enforcement, industry and academia

NIJ ECTCoE

Proposed Deliverables:

- Identifying technologies and operational requirements to meet criminal justice needs
- Support NIJ's research and development programs
- Conduct and publish a study based on empirical data to comprehensively identify the impact of electronic crime and digital evidence on State and local law enforcement
- Conduct and publish a study based on empirical data on the total number of cell phones in use and forensic solutions available
- Testing, evaluating and demonstrating electronic crime and digital evidence technologies for criminal justice use
- Supporting the adoption of new technology by the criminal justice community
- Developing technology guidelines
- Providing technology assistance & support to criminal justice community on a national basis

NIJ ECTCoE

Progress to Date:

- Identifying technologies and operational requirements to meet criminal justice needs
  - –ECTCoE has hosted the Electronic Crime TWG Meetings and identified technologies and operational requirements and evaluated projects in progress
- Support NIJ's research and development programs
  - –ECTCoE has conducted testing and evaluation on NIJ funded projects and produced reports to facilitate informed decision making
- Conduct and publish a study based on empirical data to comprehensively identify the impact of electronic crime and digital evidence on State and local law enforcement
  - –ECTCoE has drafted a plan for the needs assessment, identified the management team, advisory panel, expert reviewers, workshop facilitators, identified workshop locations and coordinators, and held two organizational meetings to train and prepare project staff
- Conduct and publish a study on the cell phones in use and the forensic solutions available
  - –ECTCoE has begun compiling the cell phones in use throughout the US and identifying the available cell phone forensic solutions
- Test, evaluate and demonstrate technologies for criminal justice use
  - –Staff has tested, evaluated and written reports on Redlight Human Image Detection; Crowbar; EnCase Portable; Mobile Phone Seizure Guide
  - –Scheduled testing & evaluation on LATT; WindowsFE; FieldSearch; SafeBoot; Lantern; TrueCrypt;

NIJ ECTCoE

Progress to Date (continued):

- Support the adoption of new technologies
  - –ECTCoE staff is scheduled to demonstrate multiple technologies at DoD Cybercrime, Techno-Security, and HTCIA
- Developing technology guidelines
  - –ECTCoE has a Publication Development Coordinator on staff responsible for publication and guideline development
  - –Work is continuing on the NIJ Publication Forensic Examination of Digital Evidence
- Providing technology assistance & support to criminal justice on a national basis
  - –ECTCoE continues to host technology workshops to demonstrate tools and technologies for criminal justice practitioners to review and provide comments for inclusion in the evaluation reports
  - –ECTCoE staff fields requests for assistance with electronic crime investigation and digital evidence collection and examination inquiries from the criminal justice community
  - –ECTCoE has developed and launched the www.ECTCoE.net electronic crime and digital evidence tool and technology resource site to provide the criminal justice community with access to NIJ funded tools and technologies, evaluation and testing reports, training information, a searchable tool and technology catalog and a searchable electronic crime investigation and digital evidence analysis resource database
  - –ECTCoE has established a secure web community on the CyberCop Portal to provide the criminal justice community with secure messaging, online criminal justice resources, a survey capability, training course proficiency test administration capability.

NIJ's Electronic Crime Technology Working Group (TWG)

- Electronic Crime TWG supports the Research, Development, Testing and Evaluation (RDT&E) process within NIJ's Office of Science and Technology.
- TWG - approximately 32 Electronic Crime, Digital Evidence & Criminal Justice Subject Matter Experts
  - responsible for identifying CJ tool & technology needs
  - identify operational requirements for law enforcement, correction, parole & probation tools & technologies
- Support NIJ's current and future RDT&E activities and ensure that future tool & technology developments address Criminal Justice high priority needs.

Tasks performed by the TWGs

- Review and validate NIJ's planned and ongoing research and development activities and recommend future technologies to address practitioner-driven needs.
- Identify additional technology needs as well as define and document operational requirements.
- Evaluate research and development programs/projects.
- Identify host agencies to serve as test-beds or "first adopters" of newly developed technologies.

TWG Recommendations / Focus Areas

NIJ ECTCOE Electronic Crime Technology Center of Excellence

- **Mobile Device Acquisition and Analysis Tools**
- **Macintosh Acquisition and Analysis Tools**
- **Network Acquisition and Analysis Tools**
- **Volatile Data Acquisition Tools**
- **Peer-To-Peer Analysis Tools**
- **Anonymous Network Analysis Tools**
- **Data Hiding and Encryption Analysis Tools**
- **Recovery of data from Damaged Hard Drives**
- **Macintosh Forensics Training**
- **Mobile Device Forensics Training**
- **Digital Evidence Recognition Training**
- **Digital Forensics Analysis Training**
- **Support Policy and Best Practices**

NIJ ECTCoE Online Resources

From the NIJ Electronic Crime Technology COE Solicitation:

NIJ is interested in having the Center implement a web-based resource center. This would include management and coordination of a Criminal Justice Electronic Crime Technology Resource Center, a password-protected Web forum that makes information available on current and emerging technologies, and practitioner information. This Web-based resource will be maintained on the NLECTC System's Justice Information Network (JUSTNET) or linked to JUSTNET.

NIJ ECTCoE Online Community and Collaboration Resource

https://cybercop.esportals.com/

ECTCoE Online Resources

http://www.ectcoe.net/h/index.php

NIJ ECTCOE
Electronic Crime Technology Center of Excellence

http://www.ojp.usdoj.gov/nij NCJ 225375

How NIJ Sets Its Research Agenda

The needs of practitioners in the field drive NIJ's RDT&E agenda.

Within NIJ's Office of Science and Technology, two specialized entities play an important role in advising its RDT&E investments: Technology Working Groups and the Law Enforcement and Corrections Technology Advisory Council.

Technology Working Groups (TWGs). A TWG is a practitioner-based committee of 10 to 20 experienced practitioners from local, state, tribal and federal agencies and laboratories associated with a particular NIJ technology investment portfolio, such as Biometrics. Each portfolio has a TWG, which identifies criminal justice technology needs within that portfolio. These portfolios and TWGs are not static; they change as priorities within the field change, as solutions are implemented or as new technologies emerge. TWG members are represented on the peer-review panels that evaluate potential solutions to address practitioner needs. Agencies from which TWG members are drawn are routinely involved in testing and evaluating the resulting solutions. The TWGs, and through them the criminal justice practitioner community, are embedded in the NIJ RDT&E process from beginning to end.

Law Enforcement and Corrections Technology Advisory Council (LECTAC). LECTAC is made up of senior criminal justice practitioners

NIJ's Technology Investment Portfolios

- Aviation.
- Biometrics.
- Body Armor.
- Communications.
- Community Corrections.
- Court Technologies.
- DNA Forensics.
- Electronic Crime.
- Explosive Device Defeat.
- General Forensics.
- Geospatial Technologies.
- Information-Led Policing.
- Institutional Corrections.
- Less-Lethal Technologies.
- Operations Research/Modeling and Simulation.
- Personal Protective Equipment.
- Pursuit Management.
- School Safety.
- Sensors and Surveillance.

NIJ ECTCOE Electronic Crime Technology Center of Excellence

NIJ ECTCOE Electronic Crime Technology Center of Excellence

High-Priority Criminal Justice Technology Needs

The following pages summarize the high-priority needs for the criminal justice field in the area of technology. These needs are organized into five functional areas:

- Protecting the Public.
- Ensuring Officer Safety.
- Confirming the Guilty and Protecting the Innocent.
- Improving the Efficiency of Justice.
- Enabling Informed Decision-Making.

CONFIRMING THE GUILTY AND PROTECTING THE INNOCENT

NIJ ECTCOE Electronic Crime Technology Center of Excellence

- Improved capability to expand the information that can be extracted from traditional types of forensic evidence and to quantify its evidentiary value, including:
  - Identification or characterization of:
    - Biological markers that may reveal more information about the source of biological evidence.
    - New substances or chemical constituents of forensic importance.
  - Improved tools for examining aged, degraded, limited, damaged, inhibited or otherwise compromised DNA evidence.
  - Tools to expand the utility of Y-chromosome and mitochondrial DNA.
  - Tools that provide a quantitative measure/statistical evaluation of forensic comparisons, including:
    - Impression evidence.
  - Physical separation of cells or components in mixtures from two or more individuals or sources, including:
    - Sperm.

- Improved capability to use and process digital evidence, including:
  - Tools to investigate the use of peer-to-peer technologies used to facilitate criminal activity, such as distribution of contraband, that address decentralized and unstructured peer-to-peer network protocols.
  - Tools that can recover system files, operating system information, applications, deleted files and unallocated space from small-scale mobile devices, such as cell phones and personal digital assistants.
  - Full data imaging solutions for networks and network-attached or -connected devices addressing:
    - Redundant Array of Independent Disks (RAID).
    - Wireless network devices, including routers, gateways, network interface cards, repeaters, switches, hubs and wirelessly connected external digital media.

IMPROVING THE EFFICIENCY OF JUSTICE

NIJ ECTCOE Electronic Crime Technology Center of Excellence

- "Intelligent" decision support systems, including:
  - Optimizing sentencing (e.g., institutionalization, probation, parole, therapy, electronic monitoring or treatment), taking into account cost, safety and recidivism issues.

  - Optimizing the way in which law enforcement agencies organize and deploy their resources, to include: patrol district, precinct and beat designs; fleet maintenance; and management and manpower scheduling.
  - Optimizing the way in which law enforcement and corrections agencies employ new technologies, such as automated vehicle locators, smart sensors, wireless mobile networks and knowledge management, in patrol and response operations.
- Improved information and data systems that link an individual's records and citations across various criminal justice databases from the time of entry into the criminal justice system.
- Web applications (services) that facilitate effective cross-jurisdiction information and data sharing and exchange. Solutions must consider the Justice Reference Architecture.
- Immersive technologies to effectively train public safety officers optimally at their stations.
- Devices providing multilingual speech translation capabilities for public safety application, including:
  - Voice.
  - Speech-to-text/text-to-speech.
- Reliable and widely applicable tools and technologies that allow faster, cheaper and less labor-intensive identification, collection, preservation and analysis of forensic evidence of all kinds and the reduction of existing case backlogs, including:
  - Improved laboratory information management systems.
  - Improved automated forensic analysis and quality assurance processes.
  - Improved solutions to address the need for increased data storage capacity to archive large-volume data sets generated in computer forensic examinations.
  - Improved solutions for extracting specific data subsets that correspond to specific files from larger data sets during analysis of unallocated space on a digital media device.

NIJ ECTCOE Electronic Crime Technology Center of Excellence

R&D Efforts

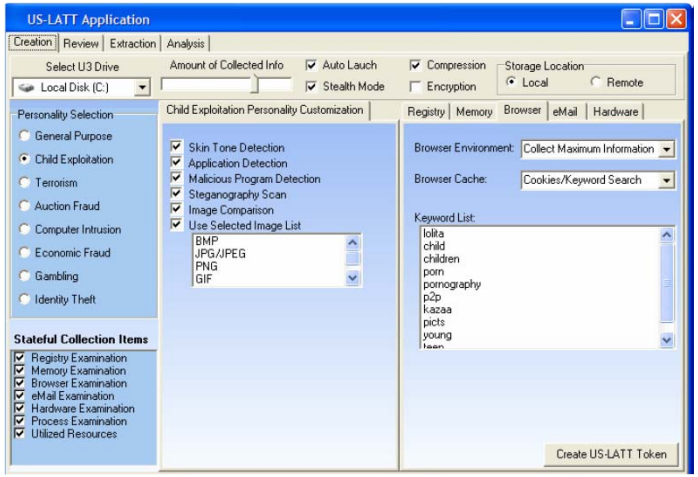
Live Computer System Capture and Triage Tools

- Live computer system capture and triage tools perform forensic examinations on live systems before they are seized (to determine the need to image live and the capability for onsite system overview). Some of these tools may perform forensic examinations during a permissible search (such as a probation search or a search with the owner's consent). These tools should capture and document:
  - Operating system information.
  - Time zone, BIOS, and hard disk drive size.
  - Encryption issues (files, motherboard, operating system).
  - Local Area Network (LAN) information (multiple computers, IP address, gateway, MAC addresses, connections).
  - Offsite storage information.
  - Random Access Memory (RAM) dump.
  - Open file dump.
  - Wireless connectivity.
  - Connected computers.
  - Connected devices and interface.
  - Web-based email.
  - Gallery viewer/multimedia player available for rapid review.
  - Chat history.
  - Instant messenger tool

Project Title: USB Live Acquisition and Triage Tool (US-LATT)
Grantee: Wetstone Technologies, Inc.
Award #: 2009-SQ-B9-K015
Program Manager/Division: Martin Novak/ISTD
Portfolio: Electronic Crime and Digital Evidence Recovery

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Concept



Operational Capability

- Tools that will perform forensic examinations on a live system before it is seized (to determine the need to image live and the capability for onsite system overview).

Deliverable:

- A fully operational US-LATT for unlimited distribution to U.S. State and Local Law Enforcement Agencies which will enhance and augment the abilities of first responders, through the use of a USB-based forensic device and software, to efficiently and effectively investigate a live computer
- Final Report to NIJ

Approach and Objectives

- Execute a field trial for USB-LATT
  - Select participants
  - Provide USB-LAT to participants
  - Incorporate participant feedback into USB-LATT
  - Finalize field trial
- Distribute final version of USB-LATT
  - Prepare for distribution
  - Distribute to State and local law enforcement
- Provide USB-LATT to the NIJ Electronic Crime Center of Excellence for independent evaluation.

Milestones and Deliverables

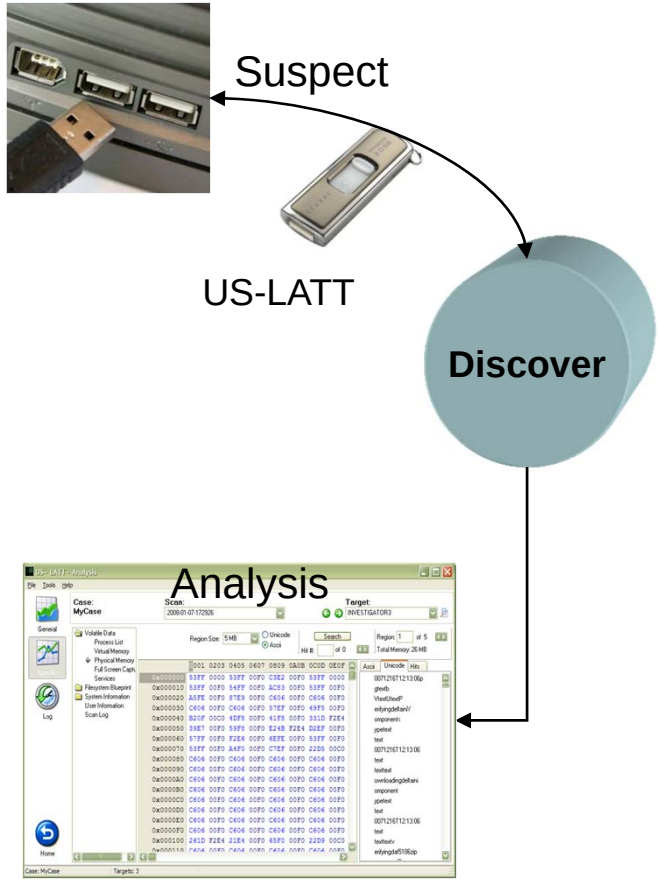
Task	Status	Completion
Field Trial	Ongoing	2QFY10
Forensic Enhancements	Not Started	3QFY10
Reporting	Ongoing	4QFY10

U3-USB-Live Acquisition and Triage Tool (US-LATT)

Product Description

- US-LATT provides investigators and first-responders with the ability to obtain live, volatile evidence from running systems under rapid response or covert scenarios. LE Officers would insert a U3 USB device that automatically captures and stores evidence from suspect computers.

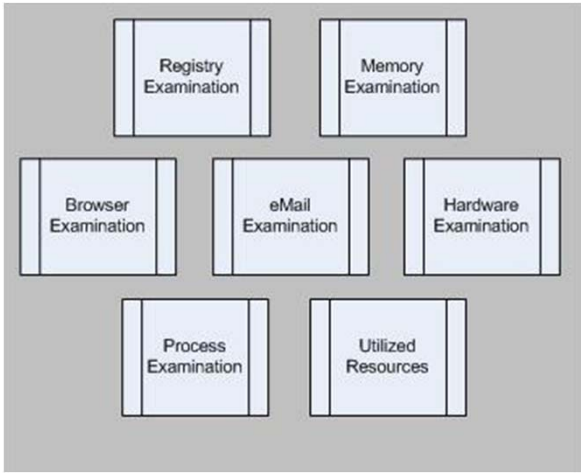
- **Criminal Justice Payoff**
  - Rapid acquisition of volatile forensic evidence
  - Forensically acquire evidence typically lost in pull the plug postmortem investigations
  - Acquire evidence of Encrypted and Steganographic File Systems and Network Attached Storage (NAS)
  - Collection of Live Physical Memory
  - Collection of Suspect Screen Shots



Mac Marshall- ATC-NY

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Concept



Operational Capability

- Tools that will perform forensic examinations on a live system before it is seized (to determine the need to image live and the capability for onsite system overview).

Deliverable:

- A memory forensics software toolkit that will assist investigators by automating memory analysis capabilities, distributed for free to State and local law enforcement

Approach and Objectives

- Make live memory analysis forensic capabilities available and useful to law enforcement through automation, visualization, and reporting features.
  - These techniques will produce important, case-relevant data for investigators that cannot be obtained from disk analysis: running applications, open files, Web browser usage, recently-used passwords, and stored encryption keys.
- Provide the capability to extend existing forensic techniques to volatile memory, to provide context for string-search results and enable in-memory file carving

Milestones and Deliverables

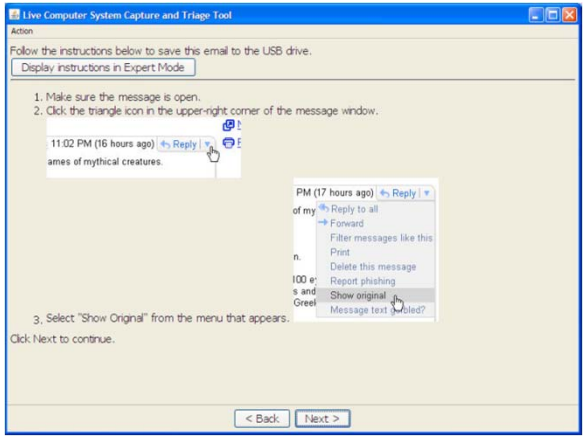
Task	Status	Completion
Develop Windows system information	Competed	1QFY10
Gather app-specific data	Ongoing	2QFY10
Develop address-space visualization	Ongoing	3QFY10
Develop automation and reporting	Not Started	4QFY10
Prepare Mem Marshal for dissemination	Not Started	4QFY10

Project Title: Cyber-investigation Law Enforcement Wizard (CLEW)

Grantee: University of Illinois at Urbana-Champaign

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Concept



Operational Capability

- Tools that perform forensic examinations during a permissible search (such as a probation search or a search with the owner's consent).

Deliverable:

- A tool that will support law enforcement with investigations into the most common E-mail, Instant Messenger, and Social Networking (e.g., Facebook) complaints.
- Tool will be available for free to State and local law enforcement.

Approach and Objectives

- Develop and prototype mechanisms to assist law enforcement with the on-site capture of important information off web-based social networking sites such as Facebook, MySpace, and Twitter. Information collected would include:
  - All mail received and sent by the user.
  - List of Friends Requests, including any pending requests.
  - Other communications, including status updates, "wall" postings, comments, etc.
  - Group memberships
  - Event Invites – List of parties, meetings and other events that the user was invited to
  - All user input info under edit profile including:

Milestones and Deliverables

Task	Status	Completion
Identify, and research existing social network data capture and analysis tools such as the MySpace *Visualizer*	Ongoing	2QFY10
Demonstrate the first prototype of the social network data capture to the City of Urbana Police Department	Not Started	3QFY10
Integrate social network data capture routine with CLEW	Not Started	4QFY10
Release CLEW for LE use	Not Started	4QFY10

Network Acquisition Tools

The development of Imaging tools for networks and network-attached devices should address one or more of the following issues:

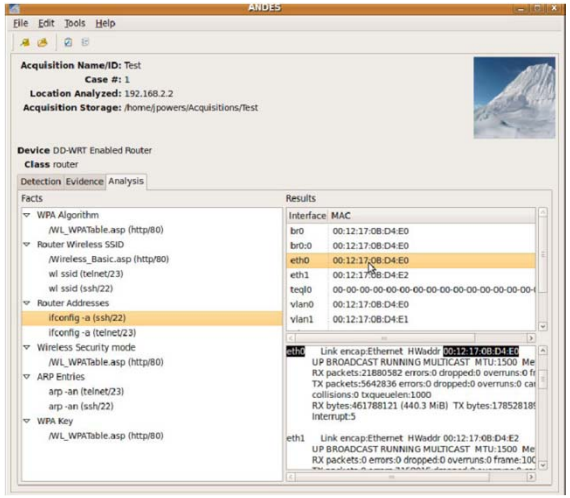
- Redundant Array of Independent Disks (RAID): A RAID is a disk subsystem that is used to increase performance and/or provide fault tolerance. A RAID uses a set of two or more ordinary hard disks and a specialized disk controller that contains the RAID functionality.
- Wireless network devices including; routers, gateways, network interface cards (NICs), repeaters, switches, hubs, and wirelessly connected external digital media.
- Network data storage devices connected via computer to the network as well as data storage devices connected directly to the network via a wired or wireless network interface or connection.

Project Title: Acquisition of Network Device Evidence System (ANDES)

Grantee: ATC-NY

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Concept



Operational Capability

- Imaging tools for networks and network-attached devices (e.g., printers, firewalls, routers, computers).

Deliverable:

- A set of software tools allowing investigators to automatically acquire and analyze forensically-relevant data from network devices without requiring device-specific training.
- Distribute for free to State and local law enforcement

Approach and Objectives

- Review best practices for the acquisition of data from network devices, including devices of different types and from different manufacturers.
- Design and develop a software tool for acquiring network device data.
  - Including the design and implementation of a configuration format that is both general and human-writable
- Usability testing with law enforcement partners and gather feedback
  - Focus on ensuring that the evidence acquisition is forensically sound.
- Make changes to ANDES based on usability testing and feedback

Milestones and Deliverables

Task	Status	Completion
Research data acquisition	Competed	1QFY10
Design and develop software	Ongoing	2QFY10
Design and develop portable device	Ongoing	3QFY10
Prepare Software for Dissemination	Not Started	4QFY10

Project Title: Windows Boot Disk for Acquiring Network Storage
Grantee: University Of Rhode Island
Award #: 2008-IJ-CX-K403
Program Manager/Division: Martin Novak/ISTD
Portfolio: Electronic Crime and Digital Evidence Recovery

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Concept

Operational Capability

- Imaging tools for networks and network-attached devices (e.g., printers, firewalls, routers, computers).

Deliverable:

- A software write blocked Windows forensic boot disk available to State and local law enforcement for free.

Approach and Objectives

- Develop a forensically sound (write blocked) Windows boot disk (CD, DVD and/or USB).
- Include the ability to open Host Protected Areas and Device Configuration Overlay areas of IDE disks.
- Develop volume support for RAID and network-attached storage in the Windows boot disk.

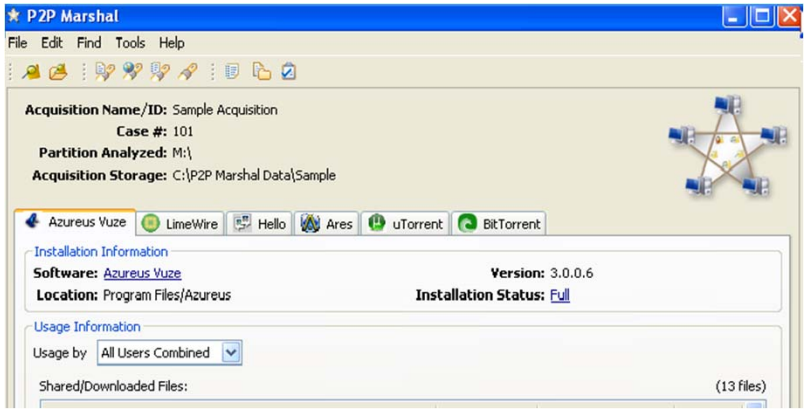
Milestones and Deliverables

Task	Status	Completion
Design Windows Forensic Boot Disk	Ongoing	Completion
Add the ability to unlock HPA/DCO disks	Ongoing	4QFY10
RAID Support	Ongoing	4QFY10
Software Packaging and dissemination	Ongoing	2QFY11

Project Title: Peer-to-Peer (P2P) Marshal
Grantee: ATC-NY

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Concept



Operational Capability

- Technologies that effectively conduct investigations into the criminal use of Peer-To-Peer (P2P) clients.

Deliverable:

- A enhanced software tool for analysis of evidence from peer-to-peer client software.
- Distribute for free to State and local law enforcement for free via web download.

Approach and Objectives

- Add new client support and enhance existing support.
  - Currently, Provides full analysis for: Ares, BitTorrent, FrostWire, LimeWire, uTorrent, and Azereus Vuze
  - Support will be added for eMule, BearShare, and DC++.
- Improve the user interface and reporting
- Enhance back-end processing and add new features
- Prepare new version of P2P Marshal for dissemination

Milestones and Deliverables

Task	Status	Completion
Add New Client Support	Ongoing	3QFY10
Improved User Interface	Ongoing	3QFY10
Enhanced Back-End Processing	Ongoing	3QFY10
Prepare Software for Dissemination	Ongoing	4QFY10
Disseminate software via web download	Ongoing	4QFY10

Data Carving Tools

- Data carving is the process of extracting data that corresponds to specific criteria from larger data sets.
- This function is frequently employed during analysis of unallocated space on a digital media device that is, areas on devices that are not currently assigned to a file but may still hold data from files that were deleted.

Project Title: Digital Forensics Analysis Search String Support
Grantee: University of Rhode Island
Award # : 2008-CE-CX-K001
Program Manager/Division: Martin Novak/ISTD
Portfolio: Electronic Crime and Digital Evidence Recovery

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Concept

[a-z#~_\.!\#$\^%&*\(\)\-]+@[a-z#_\]+\.(com)|(biz)|(de)|(edu)|(gov)|(info)|(mil)|(net)|(org)|(tv)|(uk)|(jp)

Note: The above "regular" expression will capture most valid E-mail addresses

Operational Capability

- Data carving tools, including search string support

Deliverable:

- Software tool to assist with search string capabilities in digital forensic analyses.
- Distribute for free to State and local law enforcement

Approach and Objectives

- Regular expression (strings with special characters) generation will be implemented by a web form where the user enters text and uses elements such as radio buttons and drop down boxes to qualify the text into regular expression elements.
- Perform a cycle of creating/editing the regular expression, testing its effectiveness, and then reediting if necessary.

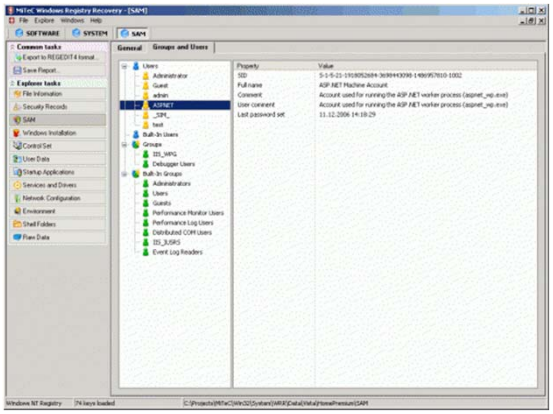
Milestones and Deliverables

Task	Status	Completion
Develop Regular Expression Test Software	Ongoing	2QFY10
Develop Regular Expression Repository	Ongoing	2QFY10
Refine and LE Test	Not Started	3QFY10
Software Documentation and Disseminate via CyberCop Portal	Not Started	4QFY10
Final Report	Not Started	4QFY10

Project Title: Registry Decoder
Grantee: Digital Forensic Solutions

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Concept



Operational Capability

- An automated forensic acquisition, examination, and analysis tools to recover, parse, and report relevant data from seized computer operating system registry keys.

Deliverable:

- An easy-to-use tool for extraction of critical information from the Microsoft Windows registry.

Approach and Objectives

- Automatically extract crucial Windows Registry information and render it in report format.
- Where possible, provide information about the meaning and relevance of extracted information.
  - e.g., "The *SANS*© Cruzer USB disk was last inserted on January 7, 2005."
- Also extract registry data from the **system restore** point facility, cross-referencing this information with current data to help an investigator understand the evolution of the system.

Note: **System Restore** is a Microsoft Windows component that allows for the rolling back of system files, registry keys, installed programs, etc., to a previous state in the event of malfunctioning or failure

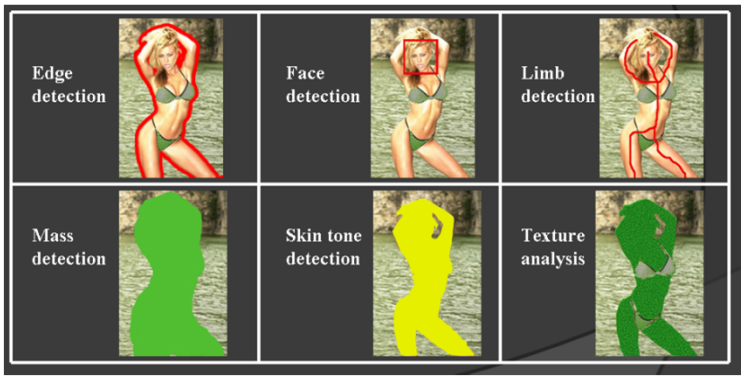
Milestones and Deliverables

Task	Status	Completion
Develop comprehensive project scope	Completed	1QFY10
Software design and implementation	Ongoing	2QFY10
Release beta version of Registry Decoder	Not Started	3QFY10
Conduct soft product launch	Not Started	4QFY10
Release official version of Registry Decoder	Not Started	1QFY11

Project Title: Automated Human Image Detection and Authentication
Grantee: University of Rhode Island
Award # : 2009-FD-CX-K215
Program Manager/Division: Martin Novak/ISTD
Portfolio: Electronic Crime and Digital Evidence Recovery

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Concept



Operational Capability

- Tools that assist law enforcement in preventing or investigating child safety issues and crimes against children via the Internet

Deliverable:

- An automated tool that will automatically detect and authenticate images of children, which will significantly reduce the time required to search for child pornography and generally improve the process for investigators.
- Disseminate to State and local law enforcement for free.

Approach and Objectives

- Refine the current detection of general pornography to detect only likely child pornography;
- Integrate the child pornography detection into a Windows forensic boot disk for triage;
- Integrate the child pornography detection into *FTK*, *EnCase*, and *X-Ways* law enforcement analysis tools in a uniform way.

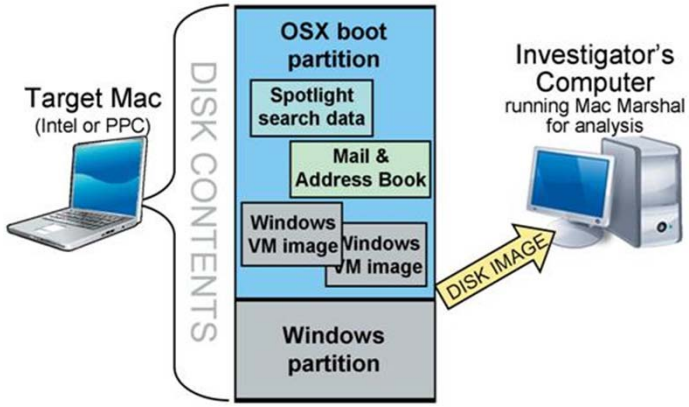
Milestones and Deliverables

Task	Status	Completion
Adding child detection capability to software	Ongoing	2QFY10
Law enforcement criteria used to tune software.	Ongoing	2QFY10
Integrate child porn scanner on SAFE boot disk	Not Started	3QFY10
Develop hash set and/or mounting of E01 feature to allow child porn scanning of disk images.	Not Started	3QFY10
Beta test triage boot disk and image file scanners with law enforcement	Not Started	4QFY10
Disseminate tools via CyberCop Portal	Not Started	4QFY10

Project Title: Mac Marshal
Grantee: ATC-NY
Award # : 2009-FD-CX-K002
Program Manager/Division: Martin Novak/ISTD
Portfolio: Electronic Crime and Digital Evidence Recovery

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Concept



Operational Capability

- Forensic examination solutions for Macintosh computers that use the Intel Core Duo processor chip which enables a dual Operating System capability using both the Mac OS X and Windows XP operating systems

Deliverable:

- A software tool, which we will distribute for free to Law Enforcement, for gathering Mac OS X-specific forensic data from target machines

Approach and Objectives

- Add new automatic analysis tools for commonly-requested forensic data
- Improve the overall usability and efficiency of Mac Marshal in crime labs' casework
- Add the ability to conduct Mac Marshal investigations on live, running systems
- Prepare the enhanced Mac Marshal tool for dissemination

Milestones and Deliverables

Task	Status	Completion
Add new Mac Marshal analysis tools	Ongoing	2QFY10
Improve the usability and efficiency of Mac Marshal in casework	Ongoing	3QFY10
Add ability to perform live investigations and gather volatile data	Not Started	3QFY10
Prepare the enhanced Mac Marshal for disseminate via web download	Not Started	4QFY10

Project Title: National Center for Media Forensics
Grantee: University of Colorado at Denver
Award #: 2008-DN-BX-K218
Program Manager/Division: Martin Novak/ISTD
Portfolio: Electronic Crime and Digital Evidence Recovery

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Concept

NCMF MEDIA FORENSICS

Operational Capability

- Digital Forensics Training

Deliverable:

- A new Master of Science in Media Forensics graduate program and continuing education for Law Enforcement.

Approach and Objectives

- Develop new methods and technologies to address the ever changing needs of law enforcement and the fight against crime;
- Serve as a primary site for a world class Master of Science degree program in Media Forensics;
- Provide training to law enforcement and related communities for professional development.

Milestones and Deliverables

Task	Status	Completion
Curriculum Development	Ongoing	3QFY10
Student Recruitment	Ongoing	3QFY10
Start Graduate Degree Program	Not Started	3QFY10
Start LE Program	Not Started	3QFY10
Update Programs as necessary	Not Started	TBD

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Training Projects

Project Title: Digital Evidence Collection Training
Grantee: International Data Forensics Solution Center

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Concept

Operational Capability

- Digital Forensic Analysis Training for State and local law enforcement

Deliverable:

- Provide Digital Evidence Collection Training to State and local law enforcement

Approach and Objectives

- Twenty-six classes will be taught in the 12 month grant funding project.
  - 26 Classes x 20 Student = 520 Total Students
- A proficiency test upon course completion and certificate of proficiency in Digital Evidence Collection for each attendee.

Milestones and Deliverables

Task	Status	Completion
Host and Support 13 DCET Courses	Ongoing	2QFY10
Host and Support 13 DCET Courses	Ongoing	1QFY11

Project Title: Computer Forensic Investigation Training
Grantee: International Data Forensics Solution Center

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Concept

Operational Capability:

- Digital Forensic Analysis Training for State and local law enforcement

Deliverable:

- Provide Computer Forensic Analysis Training to State and local law enforcement

Approach and Objectives

- Conduct the two-day CFIT classes twice a month for a twelve-month period under this grant
  - 20 Students per Class x 24 Classes = 480 Total Students
- Students who attend this training course as part of this project will receive licensed and fully functional copies of DataLifter v2.0, File Extractor Pro and DataLifter.net Bonus Tools, a collection of tools designed for the Computer Forensic Investigator.

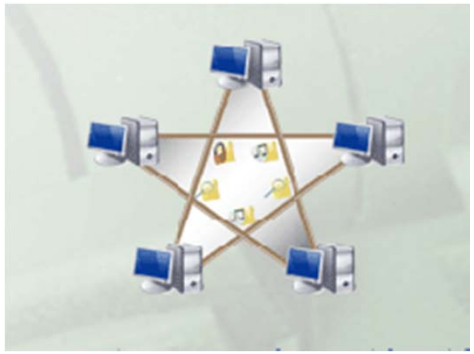
Milestones and Deliverables

Task	Status	Completion
Host and Support 12 CFIT Courses	Ongoing	2QFY10
Host and Support 12 CFIT Courses	Ongoing	1QFY11

Project Title: P2P Marshal Forensic Training
Grantee: ATC-NY

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Concept



Operational Capability

- Digital Forensic Analysis Training for State and local law enforcement

Deliverable:

- Provide training to State and local law enforcement on P2P Marshal

Approach and Objectives

- Hold 10-12 1-day training courses each year, which will each accommodate 20-45 students.
- On average, given 10 courses with 25 trainees, that would be 250 people trained per year.
- Currently, ATC-NY provides a certificate of completion. They are in the process of getting this training accredited for in-service hours.

Milestones and Deliverables

Task	Status	Completion
Prepare for and deliver P2P Marshal Forensic Training	Ongoing	4QFY10
Enhance training course	Ongoing	4QFY10
Develop Trainer's Kit	Not Started	1QFY11
Management and Reporting	Not Started	1QFY11

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Standards & Outreach

Project Title: Cyber and Electronic Crime Policy Project
Grantee: NGA – Center for Best Practices

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Concept

Operational Capability

- Inform policy-makers and decision-makers at the State and local level with regard to issues related to Electronic Crime

Overall deliverable:

- Educate governors and other high-level state policymakers on recent advancements in forensic sciences and their potential impact on state cyber and electronic crime policy.

Approach and Objectives

- Educating governors and other state policymakers on advances in the field of forensic sciences and their potential impact on state cyber and electronic crime policy;
- Providing a nexus between NIJ-supported research and state policy development; and
- Enhancing state capacity for keeping pace with significant advances in technology.

Milestones and Deliverables

Task	Status	Completion
Convene Working Group Meeting	Ongoing	2QFY10
Produce Two Working Papers	Not Started	4QFY10
Executive policy forum for governors' advisors and key state policymakers	Not Started	3QFY10
Webcasts	Not Started	4QFY10
Technical Assistance	Not Started	4QFY10

Transitions and Accomplishments

- **Transitions**
  - P2P Marshal (ATC-NY) available to LE agencies via web download
  - USB-LATT (WetStone Technologies) beta testing with app. 30 Law Enforcement Agencies completed, final modifications are being completed for deployment free of charge to law enforcement
  - Algorithms from URI Automated Steganograpy Detection integrated with *Steganos*, a WetStone Technologies product that is free to State and local law enforcement
  - BK Forensics completed the development of SIM analyzer lite and SIM analyzer Pro. Both software products are now available for free to State and local law enforcement.
  - Mac Marshal (ATC-NY) available to State and local law enforcement agencies via web download

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Convergence of Technology and Criminal Investigations

Peterson Trial Turns to Computer Evidence

Monday August 30, 2004

Last week's testimony in the Scott Peterson double-murder trial ended with a cross-examination of Detective Lydell Wall of the Stanislaus County Sheriff's Department about information that investigators found on the hard drives of Peterson's computers.

Wall testified earlier in the month that Peterson began searching for information about used fishing boats on Dec. 7, 2002, the day after he was confronted by Amber Frey about lying about his marital status. Wall testified that Peterson searched for information on used boats, fishing information, currents in San Francisco Bay and boat ramps in the area.

Defense attorney Mark Geragos attempted to show that Peterson actually began looking online for fishing information on Dec. 5, the day before the confrontation with Amber Frey, but Wall would not confirm that date.

As the trial continues this week, testimony is expected to center around dog-tracking evidence. Prosecutors claim that search dogs picked up Laci Peterson's scent at the Berkeley marina where Peterson supposedly launched his solo fishing trip the day she disappeared.

http://crime.about.com/b/2004/08/30/peterson-trial-turns-to-computer-evidence.htm

WICHITA, Kan., March 4, 2005

Computer Trail Led To BTK Suspect

Floppy Disk, DNA, Video Aided In Serial Killer Suspect's Arrest

By Dan Collins

Font size | Print | E-mail | Share

A newspaper with a headline about the BTK arrest lies in the front yard of Dennis Rader's home in Park City, Kan. (AP)

INTERACTIVE
The BTK Killer
A look at some of the lives snuffed out by Kansas' BTK Strangler and a timeline of the murders.

INTERACTIVE
Serial Killers & Mass Murder
Meet some of the world's worst killers, find out how some have gotten caught and what some have said about their crimes.

(CBS/AP) Dennis Rader came to his pastor in January with a floppy disk, saying he had the agenda of a church council meeting and needed to run off copies on a printer. The pastor obliged.

The head of Christ Lutheran Church inserted the disk into a computer, thinking it was nothing out of the ordinary. But that routine act may have cracked the BTK serial killer case.

Last Friday, four law enforcement officers came to Pastor Michael Clark's church with a search warrant and asked who had access to the computer. An electronic imprint in a disk sent to a Wichita TV station by the BTK killer had been traced to the church.

The officers, speaking softly but firmly, then said Rader had been arrested as the suspected BTK killer.

The pastor was stunned. Three times, he asked them to repeat it. "The world changed that very moment," Clark would later tell his congregation.

A computer disk appears to be among the key pieces of evidence that led police to Rader, the 59-year-old church council president and former Cub Scout leader who was charged Tuesday with 10 murders in the BTK killings that terrorized this city over three decades.

Though police have been tightlipped about why they believe Rader is the BTK killer — the judge in the case has ordered the files that explain why police arrested Rader sealed — some details of the evidence against him have emerged. Among them: the disk, DNA samples, surveillance and mocking letters with clues and grisly souvenirs.

"This was a police case that covered the span of three decades, and I don't think there's any one thing that would have cracked the case," said Richard LaMunyon, a former Wichita police chief who ran the department during most of the BTK killings.

http://www.cbsnews.com/stories/2005/03/04/national/main678013.shtml

Melanie McGuire Sentenced to Life in Prison for Murdering and Dismembering Her Husband in 2004

Woodbridge Man Found in Three Suitcases in Chesapeake Bay

NEW BRUNSWICK – Attorney General Anne Milgram and Criminal Justice Director Gregory A. Paw announced that Melanie McGuire was sentenced to life in prison today for the 2004 shooting death of her husband, William McGuire, whose severed remains were found in three suitcases along the Virginia coast.

Superior Court Judge Frederick P. DeVesa sentenced Melanie McGuire to life in prison for the murder, plus an additional five years for perjury to be served consecutively. The sentence means that McGuire, 34, must serve 66 years without possibility of parole.

McGuire was found guilty on April 23 by a Middlesex County jury following a seven-week trial before Judge DeVesa in Middlesex County. Assistant Attorney General Patricia Prezioso and Deputy Attorney General Christopher Romanyshyn prosecuted the case.

The jury convicted McGuire of killing her husband, cutting up his body and dumping his remains in the Chesapeake Bay. She also was found guilty of possession of a firearm for an unlawful purpose and perjury. McGuire committed perjury when, in an effort to cover up her crime, she sought a restraining order against her husband in Family Court two days after he disappeared, falsely claiming that he assaulted her and stormed out of their apartment.

"We are pleased that Judge DeVesa imposed life for this heinous and brutal murder," said Attorney General Milgram. "Justice for the victim and his loved ones demanded it. This was an extremely complex case, but justice was served thanks to a painstaking investigation by the State Police Major Crime Unit and the Division of Criminal Justice, and a phenomenal prosecution by our trial attorneys Patti Prezioso and Chris Romanyshyn."

"Melanie McGuire meticulously planned this vicious murder, researching her plans on the Internet and going to Pennsylvania to illegally purchase a gun two days before the victim disappeared," said Director Paw. "Fortunately, our investigators were even more determined and meticulous in tracking down the evidence and solving this horrible crime."

"This was a well-researched, calculated, execution of a murder," said Assistant Attorney General Prezioso. "I am relieved, on behalf of the state, that Melanie McGuire will remain in prison for the rest of her life."

Under the state's No Early Release Act, a life sentence is defined as 75 years for purposes of calculating the term of parole ineligibility. McGuire must serve 85 percent of that sentence, or

NIJ ECTCOE Electronic Crime Technology Center of Excellence

http://www.nj.gov/oag/newsreleases07/pr20070719a.html

NIJ Journal No. 254 • July 2006

Digital Evidence: How Law Enforcement Can Level the Playing Field With Criminals

by Nancy Ritter

About the Author
Nancy Ritter is a writer/editor at the National Institute of Justice.

The need for State and local police departments to leap ahead in the war on cyber-crime and develop procedures for identifying and processing electronic evidence is urgent. Yet, progress continues to be slow.

"At the rate we're going now, law enforcement is going to fall so far behind the electronic technology curve that, in a couple of years, we will *never* catch up," says Bob O'Leary, a former New Jersey detective, who heads up the Electronic Crimes Partnership Initiative (ECPI).

Funded by the National Institute of Justice, ECPI is a multidisciplinary team of professionals committed to enhancing law enforcement officers' ability to solve computer crimes. ECPI draws on the skills of a coalition of experts from law enforcement, academia, the government, and the private sector. The experts at ECPI teach police officers to solve computer crimes (such as using the Internet for child pornography) and to develop digital evidence (from computers or cell phones, for example) in crimes like rape and murder.[1] By educating law enforcement professionals on the myriad ways computers can facilitate criminal acts, the group seeks to help officers conduct more sophisticated investigations that will build stronger cases and lead to more convictions.

The Importance of Cyber Education

Each day, State and local law enforcement officers must identify, gather, and analyze both physical and electronic evidence in a wide range of cases. Most police officers are skilled at recognizing physical evidence in such cases, but many have never been trained to recognize the existence or importance of electronic evidence in solving a crime or building a winning case.

NIJ ECTCOE Electronic Crime Technology Center of Excellence

http://www.ojp.usdoj.gov/nij/journals/254/digital_evidence.html

Cell phone photos help N.C. police ID rape suspects

By Thomasi McDonald
The News & Observer

RALEIGH, N.C. — Police say images snapped with a Motorola cell phone helped them identify two of the three young men they think participated in an hours-long sexual assault of a minor at a North Raleigh apartment this month.

Police would not discuss how they obtained the phone or to whom it belonged.

"This is still under investigation," police spokesman Jim Sughrue said Tuesday. "We have warrants for a third person that's still out there."

Jose Eduardo Vidal Vidal, 26, of 609-A Van Thomas Drive and Kevin Acosta, 17, of 7008-H Woodbend Drive have each been charged with one count of first-degree forcible sexual offense and first-degree sexual exploitation of a minor, police reported.

Police are still searching for the third man, Renan Delafuente Jimenec, 30, who also resides at 609-A Van Thomas Drive and has been charged with the same offenses, Sughrue said.

Vidal Vidal was taken into custody Feb. 17 after police arrested him on one count of contributing to the delinquency of a minor by providing alcohol, Sughrue said. Vidal Vidal was charged with the more serious offenses Thursday after further police investigation, Sughrue said.

Acosta was arrested Monday and immediately subjected to a search warrant ordering him to submit a rape kit: blood, head and pubic hair, and saliva, according to the warrant made public Tuesday.

Police think the sexual assaults took place at Vidal Vidal and Jimenec's apartment off Six Forks Road, according to the search warrant. Investigators talked with the girl at WakeMed, and she told them the assaults began late Feb. 15 and continued until the next morning, according to the search warrant.

Investigators would not say why the girl was at the apartment or how she knew the three men charged with assaulting her.

NIJ ECTCOE Electronic Crime Technology Center of Excellence

http://www.policeone.com/investigations/articles/1665690-Cell-phone-photos-help-N-C-police-ID-rape-suspects/

ABOUT INSIDE DATELINE

Inside Dateline is your Web line into Studio 3B, providing you with a personal behind-the-scenes look at how we bring you our stories.

Whether it's a gripping crime tale, a hidden camera investigation, or a celebrity newsmaker profile -- Dateline correspondents and producers spend days, months, and sometimes even years researching and reporting the story. Learn more about what goes on inside our investigations, and find out more about some of the people we've met.

Ann Curry hosts Dateline. Dateline's producers, correspondents and host post here often. Previews to upcoming stories, more information on our reports, and follow-ups can be found on this blog.

CELL PHONE FORENSICS

Posted: Tuesday, January 23, 2007 2:10 PM by Dateline Editor

Filed Under: Crime, Behind The Scenes

by Maite Amorebieta, Dateline assistant producer

Welcome to the age of cell phone forensics.

More and more it seems cell phone evidence is being used in criminal trials. And in the Piper Rountree case, it was key.

Often, cell phone records are used in court to establish people's movements. How? Well, what most people forget, with all that these devices do these days, is that cell phones are really just two-way radios, albeit sophisticated ones.

Cell phones are constantly communicating with a network, sending pings to the nearest transmission tower, which allows your calls to be routed correctly.

Multiple antennas are tracking your phone's signal, since each tower only covers a few square miles. But, as you move, your call travels with you and is handed off to the base station receiving the strongest signal from your phone. The carrier keeps records of which towers the phone has contacted or pinged, and when. Which means a cell phone's position over time can be tracked within a few hundred yards. In urban areas with many towers, a phone can be tracked almost to the block. And as most phones become equipped with GPS chips, they only need to be turned ON to pinpoint your location in real time!

Technology is so good that hand-offs are unnoticed. But, the price we pay is that our phone calls leave a trail.
And the trail left by Piper Rountree's cell phone threatened to convict her. On the day of Fred Jablin's murder, lead detective Coby Kelley got a warrant for Piper's cell phone records. Within hours, the police were able to place that phone in the Richmond area at the time of Fred's murder and then tracked it heading east on I-64 toward Norfolk airport.

Then, the phone stopped communicating. But, once it was out of the dead zone, the phone records placed Piper's phone in Baltimore. Upon further investigation, police learned that a passenger with the last name of

NIJ ECTCOE Electronic Crime Technology Center of Excellence

http://insidedateline.msnbc.msn.com/archive/2007/01/23/39096.aspx

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Sexting

the act of sharing nude or partially nude photos via cell phone text message – technically MMS -

Jan. 15, 2009

"Sexting" Shockingly Common Among Teens

Latest Case Involves Three Teen Girls In Pa. Who Sent Nude Pics To Three Boys

Font size | Print | E-mail | Share | 373 Comments

VIDEO

Dangers Of Teen 'Sex-ting'

What teens call "sex-ting" is the act of sharing nude or partially nude photos via cell phone text message. As Harry Smith reports, few realize they are breaking the law.

Actress Vanessa Hudgens learned that innappropriate photos can end up in places you never intended them to. (CBS)

(CBS/ AP) While it may be shocking, the practice of "sexting" - sending nude pictures via text message - is not unusual, especially for high schoolers around the country.

This week, three teenage girls who allegedly sent nude or semi-nude cell phone pictures of themselves, and three male classmates in a western Pennsylvania high school who received them, are charged with child pornography.

In October a Texas eighth-grader spent the night in a juvenile detention center after his football coach found a nude picture on his cell phone that a fellow student sent him.

Roughly 20 percent of teens admit to participating in "sexting," according to a **nationwide survey (pdf)** by the National Campaign to Support Teen and Unplanned Pregnancy.

"This is a serious felony. They could be facing many years in prison," **CBS News legal analyst Lisa Bloom** said of the six teens in Pennsylvania.

But, **Bloom** added, "What are we going to do, lock up 20 percent of America's teens?"

Police in Greensburg, about 30 miles east of Pittsburgh, say the girls are 14 or 15 and the boys charged with receiving the photos are 16 or 17. None are being identified because most criminal cases in Pennsylvania juvenile courts are not public.

Police say they first learned about the pictures in October. They say a student had a phone turned on in class, a violation of school policy, which prompted an administrator to confiscate the phone and subsequently find the pictures, reports **CBS station KDKA-TV**.

NIJ ECTCOE Electronic Crime Technology Center of Excellence

http://www.cbsnews.com/stories/2009/01/15/national/main4723161.shtml

Her teen committed suicide over 'sexting'

Cynthia Logan's daughter was taunted about photo she sent to boyfriend

By Mike Celizic
TODAYshow.com contributor
updated 9:26 a.m. ET, Fri., March. 6, 2009

The image was blurred and the voice distorted, but the words spoken by a young Ohio woman are haunting. She had sent nude pictures of herself to a boyfriend. When they broke up, he sent them to other high school girls. The girls were harassing her, calling her a slut and a whore. She was miserable and depressed, afraid even to go to school.

And now Jesse Logan was going on a Cincinnati television station to tell her story. Her purpose was simple: "I just want to make sure no one else will have to go through this again."

The interview was in May 2008. Two months later, Jessica Logan hanged herself in her bedroom. She was 18.

Story continues below ↓

http://today.msnbc.msn.com/id/29546030/

Pew Internet

Pew Internet & American Life Project

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Teens and Sexting
How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging.
December 2009

http://www.ncdsv.org/images/PewInternet_TeensAndSexting_12-2009.pdf

Findings:

- 4% of cell-owning teens ages 12-17 say they have sent sexually suggestive nude or nearly nude images of themselves to someone else via text messaging
- 15% of cell-owning teens ages 12-17 say they have received sexually suggestive nude or nearly nude images of someone they know via text messaging on their cell phone.
- Older teens are much more likely to send and receive these images; 8% of 17-year olds with cell phones have sent a sexually provocative image by text and 30% have received a nude or nearly nude image on their phone.
- The teens who pay their own phone bills are more likely to send “sexts”: 17% of teens who pay for all of the costs associated with their cell phones send sexually suggestive images via text; just 3% of teens who do not pay for, or only pay for a portion of the cost of the cell phone send these images.

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Focus groups revealed that there are three main scenarios for sexting:

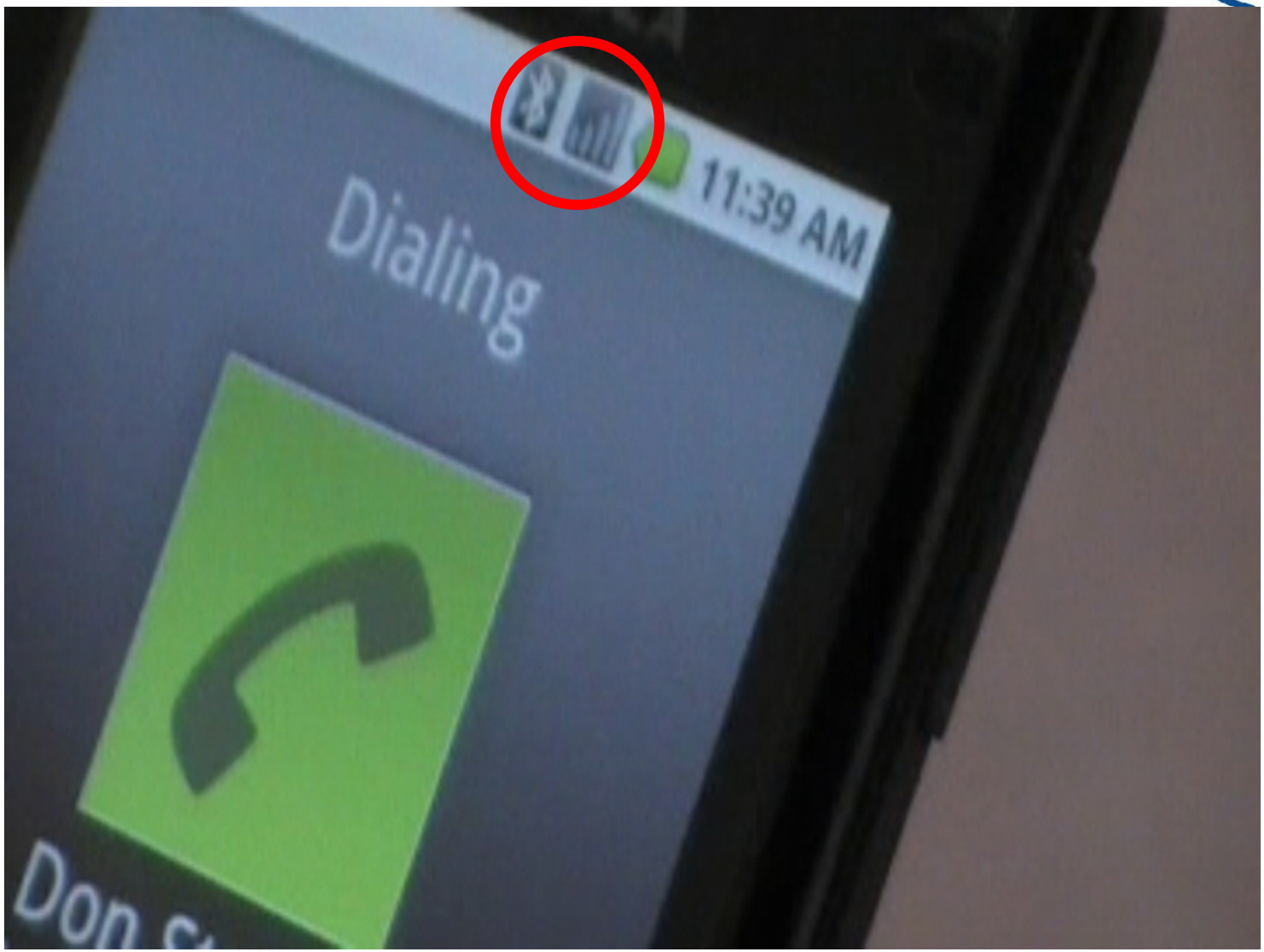
1) exchange of images solely between two romantic partners;
2) exchanges between partners that are shared with others outside the relationship and
3) exchanges between people who are not yet in a relationship, but where at least one person hopes to be.

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Technology Resources for Criminal Justice

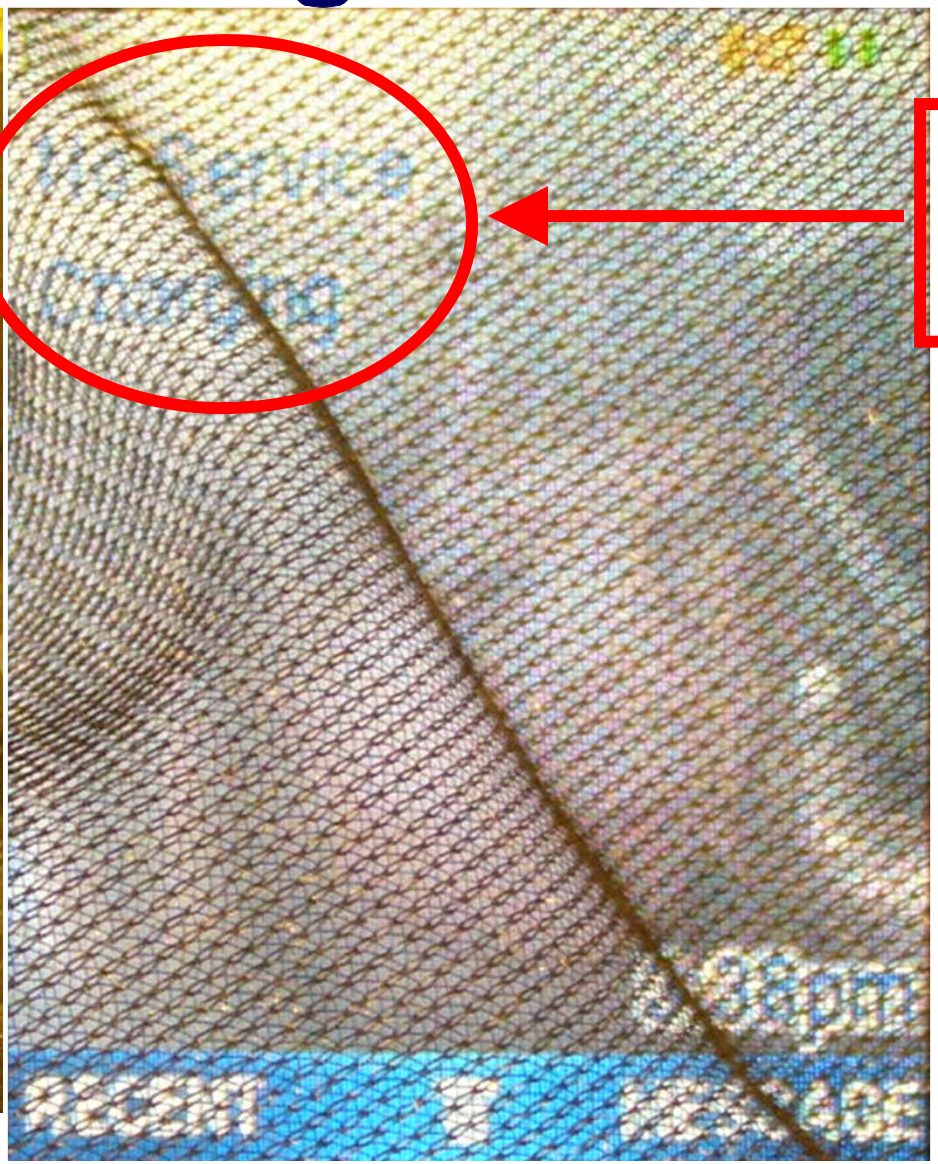
NIJ ECTCOE Electronic Crime Technology Center of Excellence

Radio Frequency (RF) signal blocking tent – prevents cell phones from accessing service providers signal


11:39 AM
Dialing

RF Shielding Material

NIJ ECTCOE Electronic Crime Technology Center of Excellence



RF Shielding Practical 1

- Partner with another attendee
- Wrap one partner's cell phone in RF Shielding material
- Check display screen – Service?
- Scroll through the menu pages-
  - Manual exam – may be the only option
- Call wrapped phone – Send text
- RF Shielding Material will block RF signal

RF Shielding Practical 2

- Partner with another attendee
- Wrap one partner's cell phone in aluminum foil
- The second partner calls the wrapped cell phone – Voice Mail? Leave message
- Unwrap the phone & check for Voice Mail
- Repeat with other partner's phone
- Aluminum foil will block RF signal

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Volatile data: information that may be lost if a computer is turned off or power is disconnected:

- Chat sessions
- Connections to other computers
- Encrypted data
- Information in RAM – Random Access Memory
- Webmail
- Running applications

Parents: Cyber Bullying Led to Teen's Suicide

Megan Meier's Parents Now Want Measures to Protect Children Online

Nov. 19, 2007

abc GMA

256 comments

Print RSS | FONT SIZE: A A A | SHARE: Email Twitter Facebook [+] More

The parents of a 13-year-old girl who believe their daughter's October 2006 suicide was the result of a cruel cyber hoax are pushing for measures to protect other children online.

Megan Meier
(Courtesy Tina Meier)

Tina and Ron Meier, who are now separated and plan to divorce, have taken up the cause of Internet safety after a bizarre twist in their daughter Megan Meier's death.

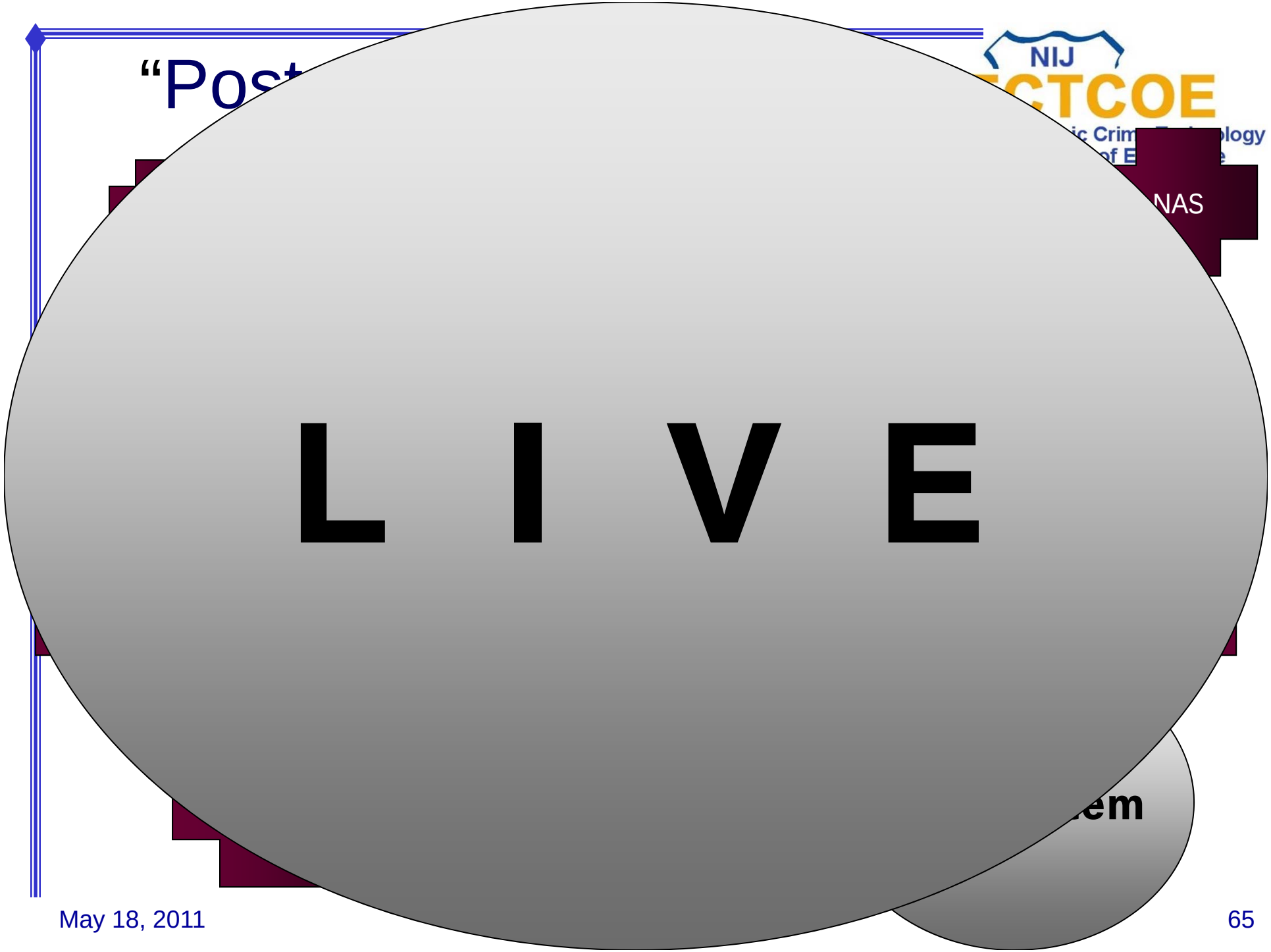
The mother of a former friend of Megan's allegedly created a fictitious profile in order to gain Megan's trust and learn what Megan was saying about her daughter. But the communication eventually turned hostile.

"There needs to be some sort of regulations out there to protect children. Parents can only be in so many places and so many times," Tina Meier said on "Good Morning America Weekend Edition" Sunday. "I wish there were regulations with these forums. There's got to be something."

The Meiers said they are unsure why someone would do such a thing.

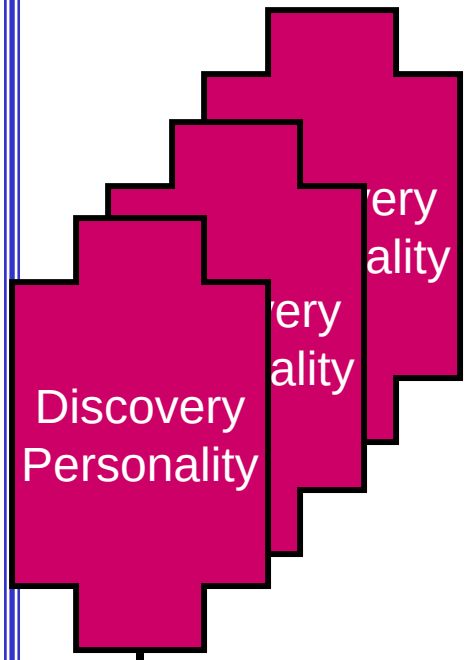
"We don't know. How do you get in the mind of somebody? We just have no idea," Tina Meier said.

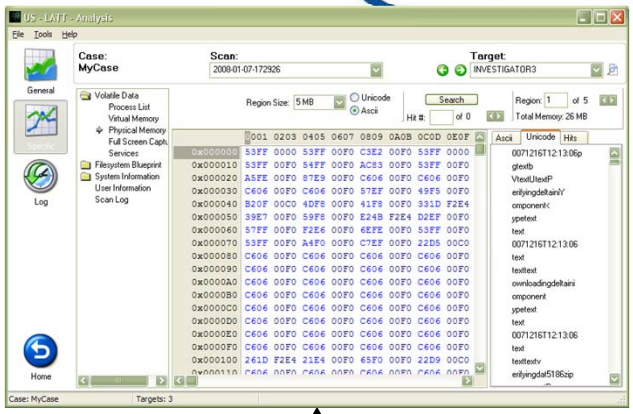
http://abcnews.go.com/GMA/story?id=3882520&page=1


NIJ
CTCOE
NAS
L I V E
em

US-LATT Architecture

NIJ ECTCOE Electronic Crime Technology Center of Excellence





Analysis and Visualization

US-LATT

Discovery Engine

XML Evidence Generation

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Other Technology Considerations

Emerging Trends

- TOR, (The Onion Router) is an Internet anonymity application. This technology enables users to hide their identity while online. Criminal activity is committed and facilitated through the exploitation of this technology. Currently, State and local law enforcement have no tools, technology or training to investigate crimes committed through the use of TOR.
- The acquisition of large digital evidence data sets using existing technologies requires hours of practitioner's time resulting in reduced productivity and case backlogs of 3 to 6 months on average. As the amount of digital evidence per case continues to grow, it will become operationally unfeasible to acquire large data sets
- Automated data acquisition and analysis technologies have yet to be developed for a large percentage of mobile devices in use in the United States

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Internet Anonymizers

- Applications developed to prevent tracking of users through Internet nodes, servers or computers
  - TOR- The Onion Router
  - Anonymizer

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Onion Routing

The Onion Routing program is made up of projects researching, designing, building, and analyzing anonymous communications systems. The focus is on practical systems for low-latency Internet-based connections that resist traffic analysis, eavesdropping, and other attacks both by outsiders (e.g. Internet routers) and insiders (Onion Routing servers themselves). Onion Routing prevents the transport medium from knowing who is communicating with whom -- the network knows only that communication is taking place. In addition, the content of the communication is hidden from eavesdroppers up to the point where the traffic leaves the OR network.

Tor: Generation 2 Onion Routing

The latest Onion Routing system is freely available and runs on most common operating systems. There is a Tor network of several hundred nodes, processing traffic from hundreds of thousands of unknown users. (The protection afforded by the system makes it difficult to determine the number of users or application connections.) Exact current and historical number of Tor nodes and global traffic volume processed are graphically depicted here. The code and documentation is available under a free license. Check out the Tor site for more details and instructions for running Tor.

The protection of Onion Routing is independent of whether the identity of the initiator of a connection (the sender) is hidden from the responder of the connection, or vice versa. The sender and receiver may wish to identify and even authenticate to each other, but do not wish others to know that they are communicating. The sender may wish to be hidden from the responder. There are many ways that a web server can deduce the identity of a client who visits it; several test sites can be used to demonstrate this. A filtering proxy can be used to reduce the threat of identifying information from a client reaching a server. Onion Routing currently makes use of the Privoxy filter for this purpose.

http://www.onion-router.net/

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Voice Over Internet Protocol (VOIP)

- Audio & optional video communications over an Internet connection
  - Wired or Wireless
  - Can be encrypted to prevent interception
  - Requires an Internet connection
    - Which can be identified

NIJ ECTCOE Electronic Crime Technology Center of Excellence

Summary

Questions?