U.S. Secret Service Investigative Strategy for Combating Cyber Crimes
• 1865 - U.S. Secret Service created to fight counterfeit currency
• 1901 - Assigned Presidential Protection duties
• 1948 - Title 18 USC Section 470-474 (Counterfeiting and Forgery)
• 1984 - Title 18 USC Section 1029 (Access Device Fraud)
• 1986 - Title 18 USC Section 1030 (Computer Fraud)
Jurisdictional History

- 1990 - Title 18 USC Section 1344 (Bank Fraud)
- 1996 - Title 18 USC Section 514 (Fictitious Obligations)
- 1998 - Title 18 USC Section 1028 (Identity Theft)
- 2001 - USA PATRIOT Act (Expanded Cyber Crime Responsibilities)
- 2004 - Title 18 USC Section 1028A (Aggravated Identity Theft)
Global Cyber Threat

• Combination of the information revolution and the effects of globalization caused the investigative mission of the Secret Service to evolve

• Advent of technology and the Internet led to a transnational “cyber criminal”

• Marked increase in the quantity, quality, and complexity of cyber crime cases targeting U.S. financial institutions and critical infrastructure
DHS Mission 4: Safeguarding and Securing Cyberspace Mission Goals and Objectives

• Ensure malicious actors are unable to effectively exploit cyberspace, impair its safe and secure use, or attack the Nation’s information infrastructure.

• Identify and evaluate the most dangerous threats to Federal civilian and private-sector networks and the Nation. Protect and make resilient information systems, networks, and personal and sensitive data.
Secret Service Investigative Strategy

• Disrupt the criminal organizations and other malicious actors engaged in high-consequence or wide-scale cyber crime.

• Manage cyber incidents from identification to resolution in a rapid and replicable manner with prompt and appropriate action.
Secret Service Investigative Strategy

• Target organized criminal groups engaged in cyber crimes
  • Target key leadership to dismantle or disrupt organized crime

• Allocate resources and personnel to maximize impact

• Foster partnerships and combine resources
  • Respond and assist local police
  • Establish formal and informal task forces
Secret Service Investigative Strategy

• Cooperate with the financial industry and academia
  • Collaborate with banks and financial institutions to identify and correct systematic weaknesses

• Develop and expand the Electronic Crimes Special Agent Program (ECSAP)

• Provide training and education to private sector and law enforcement
Multi-agency Approach to Combating Cyber Crime

- Electronic Crimes Special Agent Program (ECSAP)
- Electronic Crimes Task Forces (ECTF)
- Cyber Intelligence Section (CIS)
- Secret Service Offices Overseas
- National Computer Forensic Institute (NCFI)
- Cell Phone Forensic Facility
- Computer Emergency Response Team (CERT-CC)
Multi-agency – DHS S&T Partnership

Partner:
• Global Cyber Security Conference
• *Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector*
• Physical Extraction and Reconstruction of Evidence from Electronic Devices (University of Tulsa)
• Evidence Extraction from Mobile Phones Using SIM Side Channels

Customer:
• Blackthorn3 GPS Forensics Tool
• TriageResponder Tool
• CyberFETCH Portal
• Disposable Cell Phone Analysis
• NAND Flash Memory Chip Analysis
• Mobile Wireless Investigations
### Multi-agency – DHS S&T Partnership

#### Burner Phone Forensics
- Mobile phones with pre-pay service are frequently used in criminal activity largely due to their ease of procurement.
- Acquiring data is challenging because most run proprietary OS and have limited external connections.
- Developing free phone unlocking tutorials for law enforcement.

#### Solid State Drive Forensics
- Increasing popularity of solid state drives (SSDs) in products such as laptops is a challenging problem for forensic investigators.
- The advanced technology behind SSDs renders traditional computer forensics techniques obsolete.
- Over 200 million units will be shipped annually by 2016.

#### Vehicle and Infotainment System Forensics
- Infotainment systems store user-related data such as recent destinations, call logs, contact lists, SMS messages, and emails.
- Information is difficult to extract and stored in a proprietary format.