



U.S. Immigration
and Customs
Enforcement

MEMORANDUM FOR: Assistant Directors
All Deputy Assistant Directors
All Special Agents in Charge

FROM: Marcy M. Forman
Director, Office of Investigations

MAR 5 2007

SUBJECT: Field Guidance on Handling Detained or Seized Electronic Media
from Persons of National Security Interest at Ports of Entry

This memorandum provides guidance and clarifies responsibilities related to the detention or seizure of electronic media from persons of national security interest at Ports of Entry (POE), and serves as a reminder of current U.S. Immigration and Customs Enforcement (ICE) policies regarding the use of border search authority as it relates to electronic media. ICE's ability to exploit this media represents a unique opportunity to collect, analyze and disseminate valuable information that directly supports the missions of ICE and the Department of Homeland Security (DHS).

BORDER SEARCHES

In accordance with customs border search authorities, pursuant to section 1582 of Title 19, United States Code, ICE may conduct routine stops and searches of merchandise and persons at the U.S. border without any individualized suspicion. Additionally, pursuant to immigration authorities found in sections 1225 and 1357 of Title 8, United States Code, ICE may inspect all aliens who apply for admission; take and consider evidence concerning the privilege of any person to enter, pass through, or reside in the United States that is material or relevant to enforcement of immigration laws; and conduct a search without a warrant of any person and the personal effects in their possession when there is reasonable cause to suspect a basis for denying admission to the United States. The objective of a border search is generally twofold: (1) to inspect for merchandise being imported contrary to law; and (2) to obtain information or evidence relating to an individual's admissibility. ICE may detain or seize anything that may be evidence of a crime or indicates criminal activity. Computers, cellular phones, and other electronic media are considered closed containers with regard to border search authority and are subject to being opened and searched by ICE. Regardless of citizenship, all persons seeking admission to the United States, and their merchandise are subject to border search. There is no requirement that this search be conducted with the knowledge of the person possessing the electronic media.

ICE may review, copy, image, detain or seize, and disseminate electronic media if a violation of law is immediately evident, if further review by ICE is needed to make such a determination, or if technical assistance (e.g., translation services) is deemed necessary. Electronic media detained or seized during a border search shall not be retained by ICE longer than is necessary to determine its relevance to furthering the law enforcement mission of ICE. Any information deemed relevant will be evaluated periodically to determine its continuing significance.

Subsequent to a border search, ICE may share obtained information relating to national security with law enforcement and intelligence agencies. It is important to note that any electronic media obtained through border search authority must be searched by ICE and deemed to be of law enforcement or intelligence interest prior to any sharing with an outside agency. Pursuant to current authorities, law enforcement information may be exchanged between the law enforcement components of DHS and other local, state, Federal, and foreign law enforcement agencies in accordance with specific agreements and other legal authorities. All requests for information from the intelligence community must be coordinated with the ICE National Security Integration Center (NSIC).

ELECTRONIC MEDIA – PERSONS OF NATIONAL SECURITY INTEREST/CONCERN

Pursuant to existing referral agreements between ICE and U.S. Customs and Border Protection (CBP), all CBP interdiction matters related to terrorism or threats to national security are referred to ICE and the local Joint Terrorism Task Force (JTTF). CBP also notifies the National Targeting Center (NTC) and, through that venue, the ICE representative at the NTC will notify the ICE JTTF duty agent in the field to respond, as appropriate, per ICE policy. In most cases, the ICE JTTF duty agent will respond to the POE to interview the subject. An ICE JTTF duty agent and/or ICE Computer Forensics Agent (CFA) may conduct a cursory search of the subject's electronic media and detain or image the electronic media to conduct a more thorough examination. (NOTE: Electronic media that contains data or images that are obviously contraband should be seized in accordance with established procedures.)

In each case, the CFA (or ICE JTTF duty agent if no CFA is available) shall document the search and/or retention of information contained on the electronic media of persons of national security interest by posting a Significant Incident Report (SIR) in the Significant Event Notification System. When electronic media is physically detained, rather than merely making a forensic image of such media, that detention should be documented in the Seized Asset and Case Tracking System, as per existing ICE policy. The TECS seizure number should be referenced in the SIR.

Due to terrorist organizations' use of sophisticated measures (embedded documents/images, passwords, etc.), and routine need for translation services, the ICE JTTF duty agent may request additional technical assistance prior to determining if the electronic media contains contraband or evidence of a violation of law. In these cases, the agent should contact NSIC to arrange for additional technical assistance or review.

Questions regarding the search, detention and/or seizure of electronic media from persons of national security interest can be directed to Program Manager (b)(6);(b)(7)(C) ICE NSIC, at (202) 616-(b)(6);(or via email at (b)(6);(b)(7)(C)



U.S. Immigration and Customs Enforcement

AUG 31 2009

MEMORANDUM FOR: Assistant Director
Deputy Assistant Directors
Special Agents in Charge

FROM: (b)(6);(b)(7)(C)
Acting Director, Office of Investigations

SUBJECT: Border Searches of Electronic Devices Directive

On August 18, 2009, Assistant Secretary John Morton issued a new directive; No. 7-6.1 entitled "Border Searches of Electronic Devices." This directive supersedes U.S. Immigration and Customs Enforcement (ICE) Directive No. 7-6.0 entitled "Border Searches of Documents and Electronic Media" with respect to electronic devices only. With the exception of the March 5, 2007, OI guidance entitled "Field Guidance on Handling Detained or Seized Electronic Devices from Persons of National Security Interest at Ports of Entry" and the December 12, 2008, OI guidance entitled "Recordkeeping Procedures Regarding Detentions of Documents and Electronic Devices," all other issuances on this subject issued by ICE prior to the date of this Directive are hereby superseded.

Border searches are a well-recognized and long-established exception to the probable cause *and* warrant requirements of the Fourth Amendment. Even so, the conduct of such border searches, as with any search, must be reasonable. A lawful border search is one that is both reasonable under the Fourth Amendment and consistent with current statutes. Under statute, border search authority is only granted to "customs officers." The term "customs officers" within ICE includes Special Agents. The primary purpose of a border search by customs officers is to search for merchandise or evidence relating to merchandise.

The Office of Investigations, in conjunction with the Office of the Principal Legal Advisor, Office of International Affairs, and Office of Professional Responsibility, has revised the current ICE Directive governing border searches to address timeframes for completing border searches of electronic devices, mechanisms to ensure the capture of reliable statistics relative to these searches, and annual auditing processes to ensure compliance with the Directive.

Questions regarding this new directive should be addressed to Acting National Security Unit Chief (b)(6);(b)(7)(C) at (202) 732-(b)(6);(or (b)(6);(b)(7)(C)



DISTRIBUTION: ICE
DIRECTIVE NO.: 7-6.1
ISSUE DATE: August 18, 2009
EFFECTIVE DATE: August 18, 2009
REVIEW DATE: August 18, 2012
SUPERSEDES: See Section 3 Below.

DIRECTIVE TITLE: BORDER SEARCHES OF ELECTRONIC DEVICES

1. PURPOSE and SCOPE.

- 1.1. This Directive provides legal guidance and establishes policy and procedures within U.S. Immigration and Customs Enforcement (ICE) with regard to border search authority to search, detain, seize, retain, and share information contained in electronic devices possessed by individuals at the border, the functional equivalent of the border, and the extended border to ensure compliance with customs, immigration, and other laws enforced by ICE. This Directive applies to searches of electronic devices of all persons arriving in, departing from, or transiting through the United States, unless specified otherwise.
- 1.2. This Directive applies to border search authority only. Nothing in this Directive limits the authority of ICE Special Agents to act pursuant to other authorities such as a warrant, a search incident to arrest, or a routine inspection of an applicant for admission.

2. **AUTHORITIES/REFERENCES.** 8 U.S.C. § 1357 and other pertinent provisions of the immigration laws and regulations; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1589a, 1595a(d), and other pertinent provisions of customs laws and regulations; 31 U.S.C. § 5317 and other pertinent provisions relating to monetary instruments; 22 U.S.C. § 401 and other laws relating to exports; and the December 12, 2008, ICE Office of Investigations (OI) guidance entitled "Recordkeeping Procedures Regarding Detentions of Documents and Electronic Devices."

3. **SUPERSEDED/CANCELLED POLICY/SUMMARY OF CHANGES.** ICE Directive No. 7-6.0 entitled "Border Searches of Documents and Electronic Media" is hereby superseded as it relates to electronic devices. Additionally, all other issuances on this subject issued by ICE prior to the date of this Directive are hereby superseded as they relate to searches of electronic devices, with the exception of the March 5, 2007, OI guidance entitled "Field Guidance on Handling Detained or Seized Electronic Media from Persons of National Security Interest at Ports of Entry" and the December 12, 2008, OI guidance entitled "Recordkeeping Procedures Regarding Detentions of Documents and Electronic Media."

Border Searches of Electronic Devices

4. **BACKGROUND.** ICE is responsible for ensuring compliance with customs, immigration, and other Federal laws at the border. To that end, Special Agents may review and analyze computers, disks, hard drives, and other electronic or digital storage devices. These searches are part of ICE's long-standing practice and are essential to enforcing the law at the United States border. Searches of electronic devices are a crucial tool for detecting information concerning terrorism, narcotics smuggling, and other national security matters; alien admissibility; contraband including child pornography; laundering monetary instruments; violations of copyright or trademark laws; and evidence of embargo violations or other import or export control laws.
5. **DEFINITIONS.** The following definitions are provided for the purposes of this Directive:
 - 5.1. **Assistance.** The use of third party analytic resources such as language processing, decryption, and subject matter expertise, to assist ICE in viewing the information contained in electronic devices or in determining the meaning, context, or value of information contained therein.
 - 5.2. **Electronic Devices.** Any item that may contain information, such as computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music players, and any other electronic or digital devices.
6. **POLICY.**
 - 6.1. ICE Special Agents acting under border search authority may search, detain, seize, retain, and share electronic devices, or information contained therein, with or without individualized suspicion, consistent with the guidelines and applicable laws set forth herein. Assistance to complete a border search may be sought from other Federal agencies and non-Federal entities, on a case by case basis, as appropriate.
 - 6.2. When U.S. Customs and Border Protection (CBP) detains, seizes, or retains electronic devices, or copies of information therefrom, and turns such over to ICE for analysis and investigation (with appropriate documentation), ICE policy will apply once it is received by ICE.
 - 6.3. Nothing in this policy limits the authority of Special Agents to make written notes or reports or to document impressions relating to a border encounter in ICE's paper or electronic recordkeeping systems.
7. **RESPONSIBILITIES.**
 - 7.1. The Directors of OI, the Office of Professional Responsibility (OPR), and the Office of International Affairs (OIA) have oversight over the implementation of the provisions of this Directive.
 - 7.2. Special Agents in Charge (SACs) and Attachés are responsible for:

Border Searches of Electronic Devices

- 1) Implementing the provisions of this Directive and ensuring that Special Agents in their area of responsibility (AOR) receive a copy of this Directive and are familiar with its contents;
 - 2) Ensuring that Special Agents in their AOR have completed any training programs relevant to border searches of electronic devices, including constitutional, privacy, civil rights, and civil liberties training related to such searches, as may be required by ICE Headquarters; and
 - 3) Maintaining appropriate mechanisms for internal audit and review of compliance with the procedures outlined in this Directive. (See "Recordkeeping Procedures Regarding Detentions of Documents and Electronic Devices" memo dated December 12, 2008.)
- 7.3. Attachés are responsible for ensuring coordination with their host countries, as appropriate, before conducting any such border search outside of the United States.
- 7.4. When ICE receives electronic devices, or copies of information therefrom, from CBP for analysis and investigation, ICE Special Agents are responsible for advising CBP of the status of any such analysis within 10 calendar days, and periodically thereafter, so that CBP records may be updated as appropriate. For example, "search ongoing"; "completed with negative results"; "returned to traveler"; or "seized as evidence of a crime."
- 7.5. Special Agents are responsible for complying with the provisions of this Directive, knowing the limits of ICE authority, using this authority judiciously, and ensuring comprehension and completion of any training programs relevant to border searches of electronic devices as may be required by ICE.
- 8. PROCEDURES.**
- 8.1. **Border Searches by ICE Special Agents.**
- 1) Authorization to Conduct Border Search. Border searches of electronic devices must be performed by an ICE Special Agent who meets the definition of "customs officer" under 19 U.S.C. § 1401(i), or another properly authorized officer with border search authority, such as a CBP Officer or Border Patrol Agent, persons cross designated by ICE as customs officers, and persons whose assistance to ICE is demanded under 19 U.S.C. § 507.
 - 2) Knowledge and Presence of the Traveler. To the extent practicable, border searches should be conducted in the presence of, or with the knowledge of, the traveler. When not practicable due to law enforcement, national security, or other operational concerns, such circumstances are to be noted by the Special Agent in appropriate ICE systems. Permitting an individual to be present in the room during a search does not necessarily mean that the individual will be permitted to witness the search itself. If permitting an individual to witness the search itself could reveal law enforcement

Border Searches of Electronic Devices

techniques or potentially compromise other operational concerns, the individual will not be permitted to observe the search.

- 3) Consent Not Needed. At no point during a border search of electronic devices is it necessary to ask the traveler for consent to search.
- 4) Continuation of the Border Search. At any point during a border search, electronic devices, or copies of information therefrom, may be detained for further review either on-site at the place of detention or at an off-site location, including a location associated with a demand for assistance from an outside agency or entity (see Section 8.4).
- 5) Originals. In the event electronic devices are detained, the Special Agent should consider whether it is appropriate to copy the information therefrom and return the device. When appropriate, given the facts and circumstances of the matter, any such device should be returned to the traveler as soon as practicable. Consultation with the Office of the Chief Counsel is recommended when determining whether to retain a device in an administrative immigration proceeding. Devices will be returned to the traveler as expeditiously as possible at the conclusion of a negative border search.

8.2. Chain of Custody.

- 1) Detentions of electronic devices. Whenever ICE detains electronic devices, or copies of information therefrom, the Special Agent will initiate the correct chain of custody form or other appropriate documentation.
- 2) Seizures of electronic devices for criminal purposes. Whenever ICE seizes electronic devices, or copies of information therefrom, the Special Agent is to enter the seizure into the appropriate ICE systems. Additionally, the seizing agent must complete the correct chain of custody form or other appropriate documentation.
- 3) Retention of electronic devices for administrative immigration purposes. Whenever ICE retains electronic devices, or copies of information therefrom, or portions thereof, for administrative immigration purposes pursuant to 8 U.S.C. § 1357, the Special Agent is to record such retention in appropriate ICE systems and is to include the location of the retained files, a summary thereof, and the purpose for retention.
- 4) Notice to traveler. Whenever ICE detains, seizes, or retains original electronic devices, the Special Agent is to provide the traveler with a copy of the applicable chain of custody form or other appropriate documentation.

8.3. Duration of Border Search.

- 1) Special Agents are to complete the search of detained electronic devices, or copies of information therefrom, in a reasonable time given the facts and circumstances of the particular search. Searches are generally to be completed within 30 calendar days of

Border Searches of Electronic Devices

the date of detention, unless circumstances exist that warrant more time. Such circumstances must be documented in the appropriate ICE systems. Any detention exceeding 30 calendar days must be approved by a Group Supervisor or equivalent, and approved again every 15 calendar days thereafter, and the specific justification for additional time documented in the appropriate ICE systems.

- 2) Special Agents seeking assistance from other Federal agencies or non-Federal entities are responsible for ensuring that the results of the assistance are received in a reasonable time (see Section 8.4(5)).
- 3) In determining "reasonable time," courts have reviewed the elapsed time between the detention and the completion of the border search, taking into account any additional facts and circumstances unique to the case. As such, ICE Special Agents are to document the progress of their searches, for devices and copies of information therefrom, and should consider the following factors:
 - a) The amount of information needing review;
 - b) Whether the traveler was deprived of his or her property and, if so, whether the traveler was given the option of continuing his or her journey with the understanding that ICE would return the property once its border search was complete or a copy could be made;
 - c) Whether assistance was sought and the type of such assistance;
 - d) Whether and when ICE followed up with the agency or entity providing assistance to ensure a timely review;
 - e) Whether the traveler has taken affirmative steps to prevent the search of his or her property in a timely fashion; and
 - f) Any unanticipated exigency that may arise.

8.4. Assistance by Other Federal Agencies and Non-Federal Entities.

- 1) Translation, Decryption, and Other Technical Assistance.
 - a) During a border search, Special Agents may encounter information in electronic devices that presents technical difficulties, is in a foreign language, and/or encrypted. To assist ICE in conducting a border search or in determining the meaning of such information, Special Agents may demand translation, decryption, and/or technical assistance from other Federal agencies or non-Federal entities.
 - b) Special Agents may demand such assistance absent individualized suspicion.
 - c) Special Agents shall document such demands in appropriate ICE systems.

Border Searches of Electronic Devices

2) Subject Matter Assistance.

- a) During a border search, Special Agents may encounter information in electronic devices that are not in a foreign language or encrypted, or that do not require other technical assistance, in accordance with Section 8.4(1), but that nevertheless requires referral to subject matter experts to determine whether the information is relevant to the laws enforced and administered by ICE. For the purpose of obtaining such subject matter expertise, Special Agents may create and transmit a copy of such information to other Federal agencies or non-Federal entities.
 - b) Special Agents may demand such assistance when they have reasonable suspicion of activities in violation of the laws enforced by ICE.
 - c) Special Agents shall document such demands in appropriate ICE systems.
- 3) Demand Letter. Unless otherwise governed by a Memorandum of Understanding or similar mechanism, each demand for assistance is to be in writing (e.g., letter or email), approved by a supervisor, and documented in the appropriate ICE systems. Demands are to detail the context of the search requested, ICE's legal parameters regarding the search, retention, and sharing of any information found during the assistance, and relevant timeframes, including those described in this Directive.
- 4) Originals. For the purpose of obtaining subject matter assistance, Special Agents may create and transmit copies of information to other Federal agencies or non-Federal entities. Original electronic devices should be transmitted only when necessary to render the demanded assistance.

5) Time for Assistance and Responses Required.

- a) Assistance is to be accomplished within a reasonable period of time in order to preserve the status of the electronic devices and the integrity of the border search.
- b) It is the responsibility of the Special Agent demanding the assistance to ensure timely responses from assisting agencies or entities and to act in accord with section 8.3 of this Directive. In addition, Special Agents shall:
 - i) Inform assisting agencies or entities that they are to provide results of assistance as expeditiously as possible;
 - ii) Ensure that assisting agencies and entities are aware that responses to ICE must include any findings, observations, and conclusions drawn from their review that may relate to the laws enforced by ICE;

Border Searches of Electronic Devices

- iii) Contact the assisting agency or entity to get a status report on the demand within the first 30 calendar days;
- iv) Remain in communication with the assisting agency or entity until results are received;
- v) Document all communications and actions in appropriate ICE systems; and
- vi) Consult with a supervisor to determine appropriate action if the timeliness of results is a concern. If a demand for assistance is revoked, the Special Agent is to ensure all electronic devices are returned to ICE as expeditiously as possible.

8.5. Retention, Sharing, Safeguarding, And Destruction.

1) By ICE

- a) **Seizure and Retention with Probable Cause.** When Special Agents determine there is probable cause of unlawful activity—based on a review of information in electronic devices or on other facts and circumstances—they may seize and retain the electronic device or copies of information therefrom, or relevant portions thereof, as authorized by law.
- b) **Retention of Information in ICE Systems.** To the extent authorized by law, ICE may retain information relevant to immigration, customs, and other law enforcement matters in ICE systems if such retention is consistent with the privacy and data protection policies of the system in which such information is retained. For example, information entered into TECS during the course of an investigation will be retained consistent with the policies governing TECS.
- c) **Sharing.** Copies of information from electronic devices, or portions thereof, which are retained in accordance with this section, may be shared by ICE with Federal, state, local, and foreign law enforcement agencies in accordance with applicable law and policy. Sharing must be in compliance with the Privacy Act and applicable ICE privacy policies, such as the ICE Search, Arrest, and Seizure System of Records Notice.
- d) **Safeguarding Data During Storage and Transmission.** ICE will appropriately safeguard information detained, copied, retained, or seized under this directive while in ICE custody and during transmission to an outside entity. Appropriate safeguards include keeping materials in locked cabinets or rooms, documenting and tracking originals and copies to ensure appropriate disposition, and appropriate safeguards during transmission such as encryption of electronic data or physical protections (e.g., locked containers). Any suspected loss or compromise of information that contains personal data detained, copied, or seized under this directive must be reported immediately to the ICE Service Desk.

Border Searches of Electronic Devices

e) **Destruction**. Copies of information from electronic devices, or portions thereof, determined to be of no relevance to ICE will be destroyed in accordance with ICE policy governing the particular form of information. Such destruction must be accomplished by the responsible Special Agent within seven business days after conclusion of the border search unless circumstances require additional time, which must be approved by a supervisor and documented in appropriate ICE systems. All destructions must be accomplished no later than 21 calendar days after conclusion of the border search.

2) **By Assisting Agencies**

a) **Retention during Assistance**. All electronic devices, whether originals or copies of information therefrom, provided to an assisting Federal agency may be retained by that agency for the period of time needed to provide the requested assistance to ICE.

b) **Return or Destruction**. At the conclusion of the requested assistance, all electronic devices and data must be returned to ICE as expeditiously as possible. In the alternative, the assisting Federal agency may certify to ICE that any copies in its possession have been destroyed or it may advise ICE in accordance with Section 8.5(2)(c). In the event that any original electronic devices were transmitted, they must not be destroyed; they are to be returned to ICE.

c) **Retention with Independent Authority**. Copies may be retained by an assisting Federal agency only if and to the extent that it has the independent legal authority to do so – for example, when the information is of national security or intelligence value. In such cases, the retaining agency must advise ICE of its decision to retain certain information on its own authority. In the event that any original electronic devices were transmitted, the assisting Federal agency may make a copy of information therefrom for its retention; however, any originals must be returned to ICE.

3) **By Non-Federal Entities**

a) ICE may provide copies of information from electronic devices to an assisting non-Federal entity, such as a private language translation or data decryption service, only for the period of time needed by that entity to render the requested assistance.

b) Upon the completion of assistance, all copies of the information in the possession of the entity must be returned to ICE as expeditiously as possible. Any latent copies of the electronic data on the systems of the non-Federal entity must also be destroyed so that recovery of the data is impractical.

8.6. Review, Handling, and Sharing of Certain Types of Information.

- 1) **Border Search.** All electronic devices crossing U.S. borders are subject to border search; a claim of privilege or personal information does not prevent the search of a traveler's information at the border. However, the nature of certain types of information are subject to special handling by Special Agents, whether through policy or laws such as the Privacy Act and the Trade Secrets Act.
- 2) **Types of Information**
 - a) **Business or Commercial Information.** If, in the course of a border search, Special Agents encounter business or commercial information, such information is to be treated as business confidential information. Depending on the nature of the information presented, the Trade Secrets Act, the Privacy Act, and other laws may specifically govern or restrict handling of the information, including criminal penalties for unauthorized disclosure.
 - b) **Legal Information.** Special Agents may encounter information that appears to be legal in nature, or an individual may assert that certain information is protected by the attorney-client or attorney work product privilege. If Special Agents suspect that the content of such a document may constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction of ICE, the ICE Office of the Chief Counsel or the appropriate U.S. Attorney's Office must be contacted before beginning or continuing a search of the document and this consultation shall be noted in appropriate ICE systems.
 - c) **Other Sensitive Information.** Other possibly sensitive information, such as medical records and work-related information carried by journalists shall be handled in accordance with all applicable federal law and ICE policy. Although there is no Federal legal privilege pertaining to the doctor-patient relationship, the inherent nature of medical information warrants special care for such records. Questions regarding the review of these materials shall be directed to the ICE Office of the Chief Counsel and this consultation shall be noted in appropriate ICE systems.
- 3) **Sharing.** Information that is determined to be protected by law as privileged or sensitive is to be handled consistent with the laws and policies governing such information.

8.7 **Measurement.** ICE Headquarters will develop appropriate mechanisms to ensure that statistics regarding border searches of electronic devices, and the results thereof, can be generated from ICE systems using data elements entered by Special Agents pursuant to this Directive.

- 8.8 **Audit.** ICE Headquarters will develop and periodically administer an auditing mechanism to review whether border searches of electronic devices are being conducted in conformity with this Directive.
9. **ATTACHMENTS.** None.
10. **NO PRIVATE RIGHT STATEMENT.** This Directive is an internal policy statement of ICE. It is not intended to, and does not create any rights, privileges, or benefits, substantive or procedural, enforceable by any party against the United States, its departments, agencies, or other entities, its officers or employees; or any other person.

Approved



John Morton
Assistant Secretary
U.S. Immigration and Customs Enforcement

U.S. CUSTOMS AND BORDER PROTECTION

CBP DIRECTIVE NO. 3340-049

DATE: August 20, 2009

ORIGINATING OFFICE: FO:TO

SUPERSEDES:

REVIEW DATE: August 2012

SUBJECT: BORDER SEARCH OF ELECTRONIC DEVICES CONTAINING INFORMATION

1 PURPOSE. To provide guidance and standard operating procedures for searching, reviewing, retaining, and sharing information contained in computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players, and any other electronic or digital devices, encountered by U.S. Customs and Border Protection (CBP) at the border, both inbound and outbound, to ensure compliance with customs, immigration, and other laws that CBP is authorized to enforce.

These searches are part of CBP's long-standing practice and are essential to enforcing the law at the U.S. border. Searches of electronic devices help detect evidence relating to terrorism and other national security matters, human and bulk cash smuggling, contraband, and child pornography. They can also reveal information about financial and commercial crimes, such as those relating to copyright, trademark and export control violations. Finally, searches at the border are often integral to a determination of admissibility under the immigration laws.

2 POLICY.

2.1 CBP will protect the rights of individuals against unreasonable search and seizure and ensure privacy protections while accomplishing its enforcement mission.

2.2 All CBP Officers, Border Patrol Agents, Air Interdiction Agents, Marine Interdiction Agents, and other employees authorized by law to perform searches at the border, the functional equivalent of the border (FEB), or the extended border shall adhere to the policy described in this Directive.

2.3 This Directive governs border search authority only. It does not limit CBP's authority to conduct other lawful searches at the border, e.g., pursuant to a warrant, consent, or incident to an arrest; it does not limit CBP's ability to record impressions relating to border encounters; it does not restrict the dissemination of information as required by applicable statutes and Executive Orders.

2.4 This Directive does not govern searches of shipments containing commercial quantities of electronic devices (e.g., a shipment of hundreds of laptop computers transiting from the factory to the distributor).

CBP Form 232C (04/03)

2.5 This Directive does not supersede *Restrictions on Importation of Seditious Matter*, Directive 2210-001A. Seditious materials encountered through a border search should continue to be handled pursuant to Directive 2210-001A or any successor thereto.

2.6 This Directive does not supersede *Processing Foreign Diplomatic and Consular Officials*, Directive 3340-032. Diplomatic and consular officials encountered at the border, the FEB, or extended border should continue to be processed pursuant to Directive 3340-032 or any successor thereto.

2.7 This Directive applies to searches performed by or at the request of CBP. With respect to searches performed by U.S. Immigration and Customs Enforcement (ICE), ICE Special Agents exercise concurrently-held border search authority that is covered by ICE's own policy and procedures. When CBP detains, seizes, or retains electronic devices, or copies of information therefrom, and turns such over to ICE for analysis and investigation (with appropriate documentation), ICE policy will apply once it is received by ICE.

3 DEFINITIONS.

3.1 Officer. A Customs and Border Protection Officer, Border Patrol Agent, Air Interdiction Agent, Marine Interdiction Agent, Internal Affairs Agent, or any other official of CBP authorized to conduct border searches.

3.2 Electronic Device. Includes any devices that may contain information, such as computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players, and any other electronic or digital devices.

3.3 Destruction. For electronic records, destruction is deleting, overwriting, or degaussing in compliance with CBP Information Systems Security Policies and Procedures Handbook, CIS HB 1400-05C.

3.4 Border Search of Information. Excludes actions taken to determine if a device functions (e.g., turning an electronic device on and off), or actions taken to determine if contraband is concealed within the device itself. The definition also excludes the review of information voluntarily provided by an individual in an electronic format (for example, when an individual voluntarily shows an e-ticket on an electronic device to an Officer).

4 AUTHORITY/REFERENCES. 8 U.S.C. 1225, 1357 and other pertinent provisions of the immigration laws and regulations; 19 U.S.C. 482, 507, 1461, 1496, 1581, 1582, 1595a(d), and other pertinent provisions of customs laws and regulations; 31 U.S.C. 5317 and other pertinent provisions relating to monetary instruments; 22 U.S.C. 401 and other laws relating to exports; Guidelines for Detention and Seizures of Pornographic Materials, Directive 4410-001B; Disclosure of Business Confidential Information to Third Parties, Directive 1450-015; Accountability and Control of Custody Receipt for Detained and Seized Property (CF6051), Directive 5240-005.

5 PROCEDURES.

5.1 Border Searches.

5.1.1 Border searches may be performed by an Officer or other individual authorized to perform or assist in such searches (e.g., under 19 U.S.C. 507).

5.1.2 In the course of a border search, with or without individualized suspicion, an Officer may examine electronic devices and may review and analyze the information encountered at the border, subject to the requirements and limitations provided herein and applicable law.

5.1.3 Searches of electronic devices will be documented in appropriate CBP systems of records and should be conducted in the presence of a supervisor. In circumstances where operational considerations prevent a supervisor from remaining present for the entire search, or where a supervisory presence is not practicable, the examining Officer shall, as soon as possible, notify the appropriate supervisor about the search and any results thereof.

5.1.4 Searches of electronic devices should be conducted in the presence of the individual whose information is being examined unless there are national security, law enforcement, or other operational considerations that make it inappropriate to permit the individual to remain present. Permitting an individual to be present in the room during a search does not necessarily mean that the individual will be permitted to witness the search itself. If permitting an individual to witness the search itself could reveal law enforcement techniques or potentially compromise other operational considerations, the individual will not be permitted to observe the search itself.

5.2 Review and Handling of Privileged or Other Sensitive Material.

5.2.1 Officers may encounter materials that appear to be legal in nature, or an individual may assert that certain information is protected by attorney-client or attorney work product privilege. Legal materials are not necessarily exempt from a border search, but they may be subject to the following special handling procedures: If an Officer suspects that the content of such a material may constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction of CBP, the Officer must seek advice from the CBP Associate/Assistant Chief Counsel before conducting a search of the material, and this consultation shall be noted in appropriate CBP systems of records. CBP counsel will coordinate with the U.S. Attorney's Office as appropriate.

5.2.2 Other possibly sensitive information, such as medical records and work-related information carried by journalists, shall be handled in accordance with any applicable federal law and CBP policy. Questions regarding the review of these materials shall be directed to the CBP Associate/Assistant Chief Counsel, and this consultation shall be noted in appropriate CBP systems of records.

5.2.3 Officers encountering business or commercial information in electronic devices shall treat such information as business confidential information and shall protect that information from unauthorized disclosure. Depending on the nature of the information presented, the Trade Secrets Act, the Privacy Act, and other laws, as well as CBP policies, may govern or restrict the handling of the information. Any questions regarding the handling of business or commercial information may be directed to the CBP Associate/Assistant Chief Counsel.

5.2.4 Information that is determined to be protected by law as privileged or sensitive will only be shared with federal agencies that have mechanisms in place to protect appropriately such information.

5.3 Detention and Review in Continuation of Border Search of Information

5.3.1 Detention and Review by CBP

An Officer may detain electronic devices, or copies of information contained therein, for a brief, reasonable period of time to perform a thorough border search. The search may take place on-site or at an off-site location, and is to be completed as expeditiously as possible. Unless extenuating circumstances exist, the detention of devices ordinarily should not exceed five (5) days.

5.3.1.1 Approval of and Time Frames for Detention. Supervisory approval is required for detaining electronic devices, or copies of information contained therein, for continuation of a border search after an individual's departure from the port or other location of detention. Port Director, Patrol Agent in Charge, or other equivalent level manager approval is required to extend any such detention beyond five (5) days. Extensions of detentions exceeding fifteen (15) days must be approved by the Director Field Operations, Chief Patrol Agent, Director, Air Operations, Director, Marine Operations, or other equivalent manager, and may be approved and re-approved in increments of no more than seven (7) days. Approvals for detention and any extension thereof shall be noted in appropriate CBP systems of records.

5.3.1.2 Destruction. Except as noted in section 5.4 or elsewhere in this Directive, if after reviewing the information pursuant to the time frames discussed in section 5.3, there is not probable cause to seize it, any copies of the information must be destroyed, and any electronic device must be returned. Upon this determination that there is no value to the information copied from the device, the copy of the information is destroyed as expeditiously as possible, but no later than seven (7) days after such determination unless circumstances require additional time, which must be approved by a supervisor and documented in an appropriate CBP system of records and which must be no later than twenty one (21) days after such determination. The destruction shall be noted in appropriate CBP systems of records.

5.3.1.3 Notification of Border Search. When a border search of information is conducted on an electronic device, and when the fact of conducting this search can be disclosed to the individual transporting the device without hampering national security or

law enforcement or other operational considerations, the individual may be notified of the purpose and authority for these types of searches, how the individual may obtain more information on reporting concerns about their search, and how the individual may seek redress from the agency if he or she feels aggrieved by a search.

5.3.1.4 Custody Receipt. If CBP determines it is necessary to detain temporarily an electronic device to continue the search, the Officer detaining the device shall issue a completed Form 6051D to the individual prior to the individual's departure.

5.3.2 Assistance by Other Federal Agencies.

5.3.2.1 The use of other federal agency analytical resources outside of CBP and ICE, such as translation, decryption, and subject matter expertise, may be needed to assist CBP in reviewing the information contained in electronic devices or to determine the meaning, context, or value of information contained in electronic devices.

5.3.2.2 Technical Assistance – With or Without Reasonable Suspicion. Officers may sometimes have technical difficulties in conducting the search of electronic devices such that technical assistance is needed to continue the border search. Also, in some cases Officers may encounter information in electronic devices that requires technical assistance to determine the meaning of such information, such as, for example, information that is in a foreign language and/or encrypted (including information that is password protected or otherwise not readily reviewable). In such situations, Officers may transmit electronic devices or copies of information contained therein to seek technical assistance from other federal agencies. Officers may seek such assistance with or without individualized suspicion.

5.3.2.3 Subject Matter Assistance by Other Federal Agencies – With Reasonable Suspicion. In addition to encountering information in electronic devices that is in a foreign language, encrypted, or requires technical assistance, Officers may encounter information that requires referral to subject matter experts in other federal agencies to determine the meaning, context, or value of information contained therein as it relates to the laws enforced and administered by CBP. Therefore, Officers may transmit electronic devices or copies of information contained therein to other federal agencies for the purpose of obtaining subject matter assistance when they have reasonable suspicion of activities in violation of the laws enforced by CBP. While many factors may result in reasonable suspicion, the presence of an individual on a government-operated and government-vetted terrorist watch list will be sufficient to create reasonable suspicion of activities in violation of the laws enforced by CBP.

5.3.2.4 Approvals for seeking translation, decryption, and subject matter assistance. Requests for translation, decryption, and subject matter assistance require supervisory approval and shall be properly documented and recorded in CBP systems of records. If an electronic device is to be detained after the individual's departure, the Officer detaining the device shall execute a Form 6051D and provide a copy to the individual

prior to the individual's departure. All transfers of the custody of the electronic device will be recorded on the Form 6051D.

5.3.2.5 Electronic devices should be transmitted only when necessary to render the requested translation, decryption, or subject matter assistance. Otherwise, a copy of such information should be transmitted in lieu of the device in accord with this Directive.

5.3.2.6 When information from an electronic device is transmitted to another federal agency for translation, decryption, or subject matter assistance, the individual will be notified of this transmission unless CBP determines, in consultation with the receiving agency or other agency as appropriate, that notification would be contrary to national security or law enforcement or other operational interests. If CBP's transmittal seeks assistance regarding possible terrorism, or if the individual is on a government-operated and government-vetted terrorist watch list, the individual will not be notified of the transmittal or his or her presence on a watch list. When notification is made to the individual, the Officer will annotate the notification in CBP systems of records and on the Form 6051D.

5.3.3 Responses and Time for Assistance

5.3.3.1 Responses Required. Agencies receiving a request for assistance in conducting a border search are to provide such assistance as expeditiously as possible. Where subject matter assistance is requested, responses should include all appropriate findings, observations, and conclusions relating to the laws enforced by CBP.

5.3.3.2 Time for Assistance. Responses from assisting agencies are expected in an expeditious manner so that CBP may complete the border search in a reasonable period of time. Unless otherwise approved by the Director Field Operations, Chief Patrol Agent, Director, Air Operations, Director, Marine Operations, or equivalent level manager, responses from an assisting agency should be received within fifteen (15) days. If the assisting agency is unable to respond in that period of time, the Director Field Operations, Chief Patrol Agent, Director, Air Operations, Director, Marine Operations, or equivalent level manager may permit extensions in increments of seven (7) days.

5.3.3.3 Revocation of a Request for Assistance. If at any time a CBP supervisor involved in a request for assistance is not satisfied with the assistance being provided, the timeliness of assistance, or any other articulable reason, the request for assistance may be revoked, and the CBP supervisor may require the assisting agency to return to CBP all electronic devices that had been provided to the assisting agency, and any copies thereof, as expeditiously as possible, except as noted in 5.4.2.3. Any such revocation shall be documented in appropriate CBP systems of records. When CBP has revoked a request for assistance because of the lack of a timely response, CBP may initiate the request with another agency pursuant to the procedures outlined in this Directive.

5.3.3.4 Destruction. Except as noted in section 5.4.1 below or elsewhere in this Directive, if after reviewing information, probable cause to seize the information does not exist, CBP will retain no copies of the information.

5.4 Retention and Sharing of Information Found in Border Searches

5.4.1 Retention and Sharing of Information Found in Border Searches

5.4.1.1 Retention with Probable Cause. Officers may seize and retain an electronic device, or copies of information from the device, when, based on a review of the electronic device encountered or on other facts and circumstances, they determine there is probable cause to believe that the device, or copy of the contents thereof, contains evidence of or is the fruit of a crime that CBP is authorized to enforce.

5.4.1.2 Retention of Information in CBP Privacy Act-Compliant Systems. Without probable cause to seize an electronic device or a copy of information contained therein, CBP may retain only information relating to immigration, customs, and other enforcement matters if such retention is consistent with the privacy and data protection standards of the system of records in which such information is retained. For example, information collected in the course of immigration processing for the purposes of present and future admissibility of an alien may be retained in the A-file, Central Index System, TECS, and/or ENFORCE or other systems as may be appropriate and consistent with the policies governing such systems.

5.4.1.3 Sharing Generally. Nothing in this Directive limits the authority of CBP to share copies of information contained in electronic devices (or portions thereof), which are retained in accordance with this Directive, with federal, state, local, and foreign law enforcement agencies to the extent consistent with applicable law and policy.

5.4.1.4 Sharing of Terrorism Information. Nothing in this Directive is intended to limit the sharing of terrorism-related information to the extent the sharing of such information is mandated by statute, Presidential Directive, or DHS policy. Consistent with 6 U.S.C. 122(d)(2) and other applicable law and policy, CBP, as a component of DHS, will promptly share any terrorism information encountered in the course of a border search with elements of the federal government responsible for analyzing terrorist threat information. In the case of such terrorism information sharing, the element receiving the information will be responsible for providing CBP with all appropriate findings, observations, and conclusions relating to the laws enforced by CBP. The receiving entity will be responsible for managing retention and disposition of information it receives in accordance with its own legal authorities and responsibilities.

5.4.1.5 Safeguarding Data During Storage and Transmission. CBP will appropriately safeguard information retained, copied, or seized under this Directive and during transmission to another federal agency. Appropriate safeguards include keeping materials in locked cabinets or rooms, documenting and tracking copies to ensure appropriate disposition, and other safeguards during transmission such as password

protection or physical protections. Any suspected loss or compromise of information that contains personal data retained, copied, or seized under this Directive must be immediately reported to the Port Director, Patrol Agent in Charge or equivalent level manager and the CBP Office of Internal Affairs.

5.4.1.6 Destruction. Except as noted in this section or elsewhere in this Directive, if after reviewing information, there exists no probable cause to seize the information, CBP will retain no copies of the information.

5.4.2 Retention by Agencies Providing Translation, Decryption, or Subject Matter Assistance

5.4.2.1 During Assistance. All electronic devices, or copies of information contained therein, provided to an assisting federal agency may be retained by that agency for the period of time needed to provide the requested assistance to CBP or in accordance with section 5.4.2.3 below.

5.4.2.2 Return or Destruction. At the conclusion of the requested assistance, all information must be returned to CBP as expeditiously as possible, and the assisting agency must advise CBP in accordance with section 5.3.3 above. In addition, the assisting federal agency should destroy all copies of the information transferred to that agency unless section 5.4.2.3 below applies. In the event that any electronic devices are transmitted, they must not be destroyed; they are to be returned to CBP unless seized by the assisting agency based on probable cause or retained per 5.4.2.3.

5.4.2.3 Retention with Independent Authority. If an assisting federal agency elects to continue to retain or seize an electronic device or information contained therein, that agency shall assume responsibility for processing the retention or seizure. Copies may be retained by an assisting federal agency only if and to the extent that it has the independent legal authority to do so—for example, when the information relates to terrorism or national security and the assisting agency is authorized by law to receive and analyze such information. In such cases, the retaining agency should advise CBP of its decision to retain information under its own authority.

5.5 Reporting Requirements

5.5.1 The Officer performing the border search of information shall be responsible for completing all after-action reporting requirements. This responsibility includes ensuring the completion of all applicable documentation such as the Form 6051D when appropriate, and creation and/or updating records in CBP systems. Reports are to be created and updated in an accurate, thorough, and timely manner. Reports must include all information related to the search through the final disposition including supervisory approvals and extensions when appropriate.

5.5.2 In instances where an electronic device or copy of information contained therein is forwarded within CBP as noted in section 5.3.1, the receiving Officer is responsible for recording all information related to the search from the point of receipt forward through the final disposition.

5.5.3 Reporting requirements for this Directive are in addition to, and do not replace, any other applicable reporting requirements.

5.6 Management Requirements

5.6.1 The duty supervisor shall ensure that the Officer completes a thorough inspection and that all notification, documentation, and reporting requirements are accomplished.

5.6.2 The appropriate CBP Second line supervisor shall approve and monitor the status of the detention of all electronic devices or copies of information contained therein.

5.6.3 The appropriate CBP Second line supervisor shall approve and monitor the status of the transfer of any electronic device or copies of information contained therein for translation, decryption, or subject matter assistance from another federal agency.

5.6.4 The Director, Field Operations, Chief Patrol Agent, Director, Air Operations, Director, Marine Operations, or equivalent level manager shall establish protocols to monitor the proper documentation and recording of searches conducted pursuant to this Directive and the detention, transfer, and final disposition of electronic devices or copies of information contained therein in order to ensure compliance with the procedures outlined in this Directive.

6 MEASUREMENT. CBP Headquarters will continue to develop and maintain appropriate mechanisms to ensure that statistics regarding border searches of electronic devices, and the results thereof, can be generated from CBP systems using data elements entered by Officers pursuant to this Directive.


7 AUDIT. CBP Management Inspection will develop and periodically administer an auditing mechanism to review whether border searches of electronic devices are being conducted in conformity with this Directive.

8 NO PRIVATE RIGHT CREATED. This Directive is an internal policy statement of U.S. Customs and Border Protection and does not create or confer any rights, privileges, or benefits on any person or party.

9 DISCLOSURE. This Directive may be shared with the public.

10. SUPERSEDES. Procedures for Border Search/Examination of Documents, Paper, and Electronic Information (July 5, 2007) and Policy Regarding Border Search of Information (July 16, 2008) to the extent they pertain to electronic devices.

(b)(6);(b)(7)(C)



TCFTP Physical Analyzer



epic.org



EPIC-17-06-13-ICE-FOIA-20181115-Supplemental-Production-pt1

2018-ICLI-00030 962

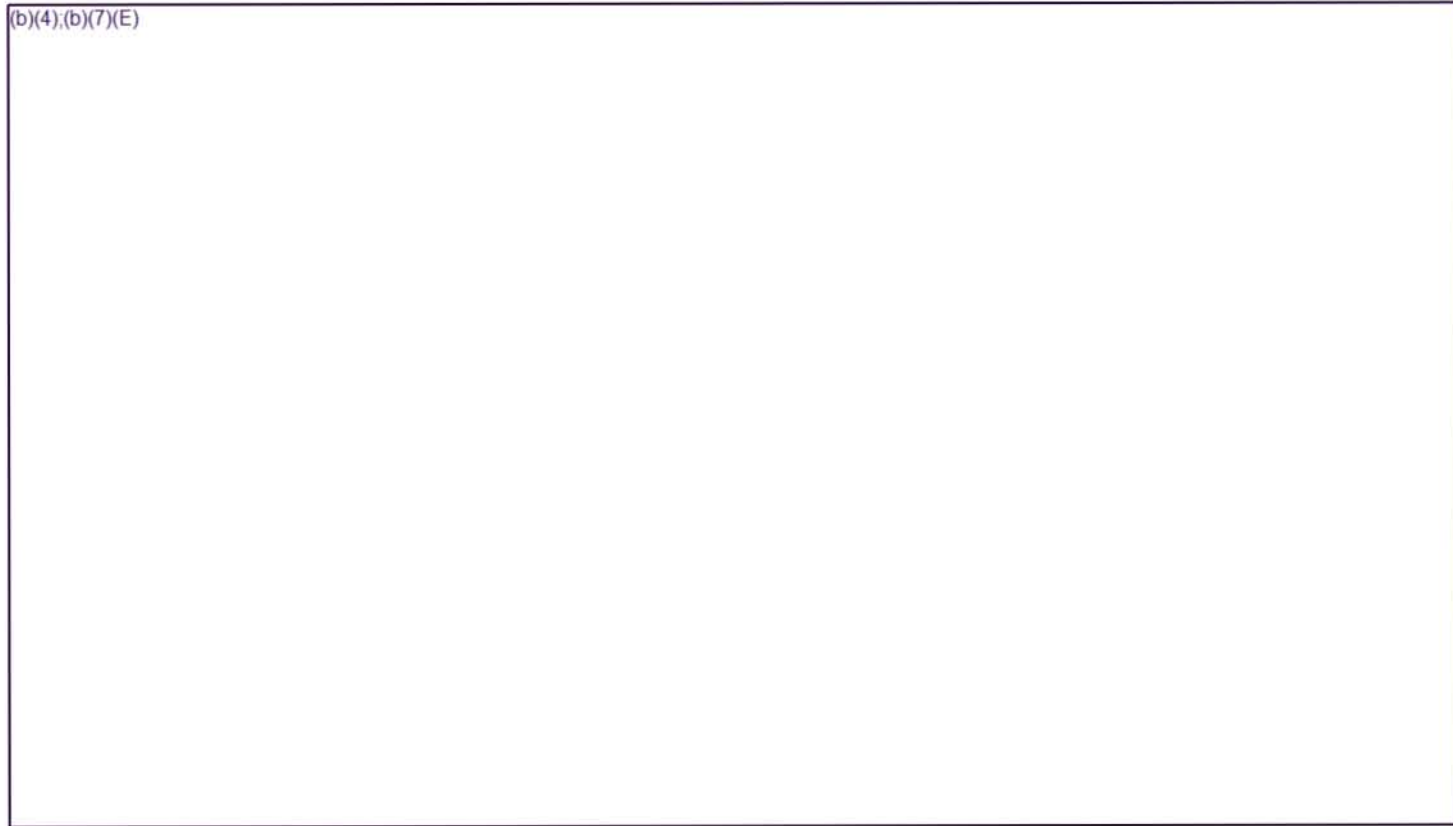


1

000962

Physical Analyzer

(b)(4);(b)(7)(E)

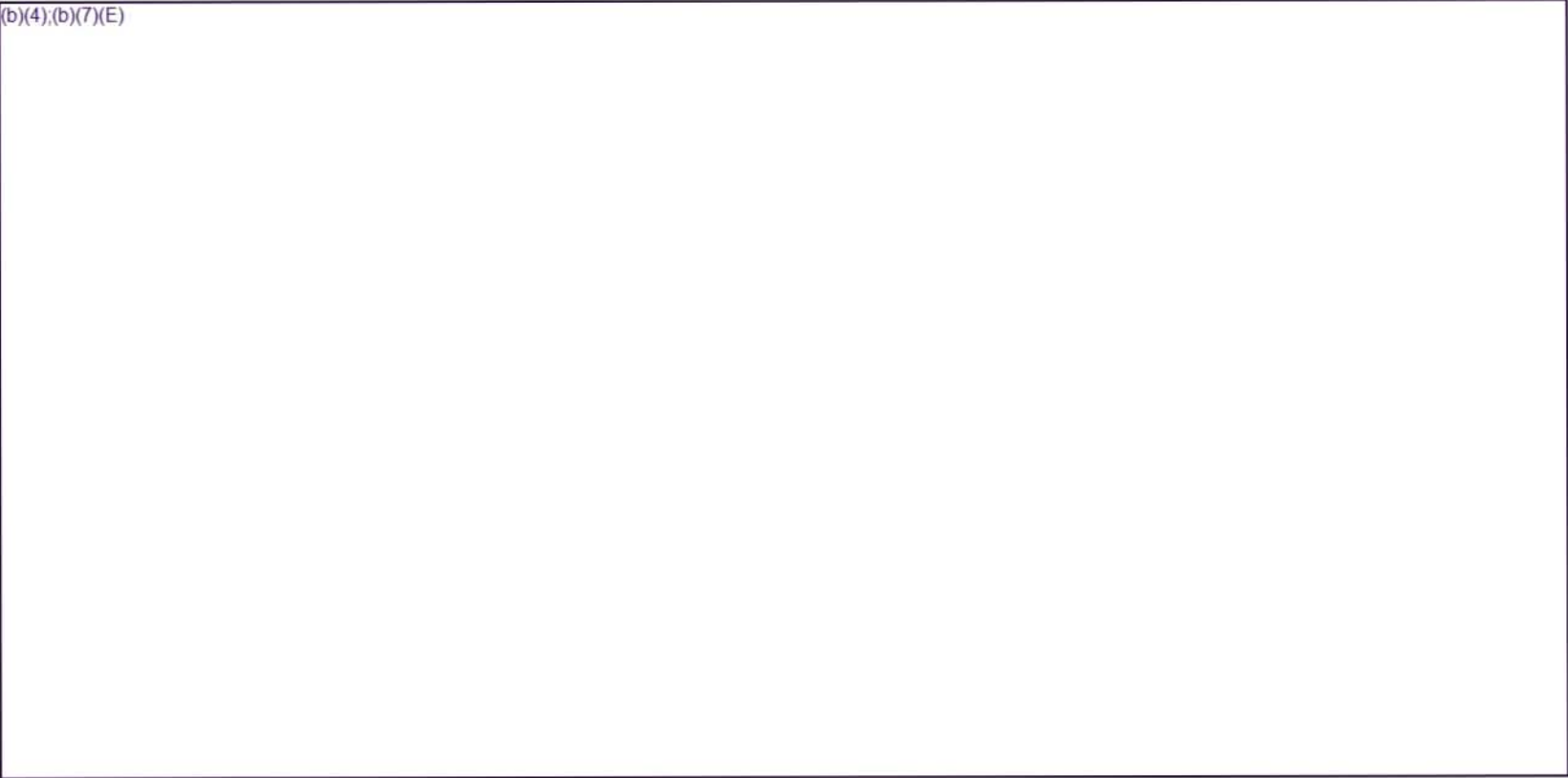


Physical Analyzer

(b)(4);(b)(7)(E)

Physical Analyzer

(b)(4);(b)(7)(E)



(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

Case Opening

Physical Analyzer

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

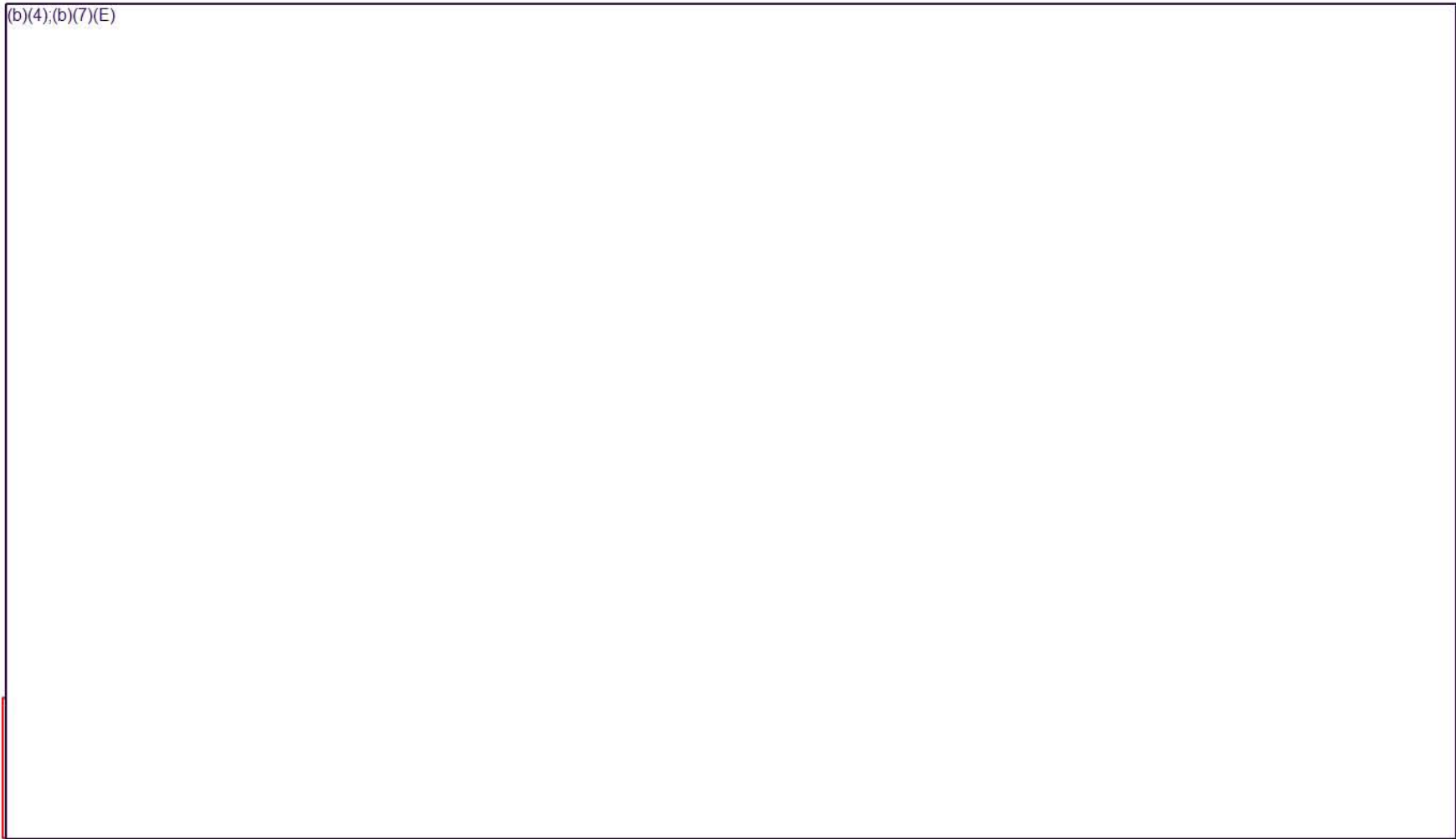
(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4),(b)(7)(E)

(b)(4),(b)(7)(E)

(b)(4);(b)(7)(E)



(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

b)(4),(b)(7)(E)

4),(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4),(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4),(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

Physical Analyzer

(b)(4);(b)(7)(E)

Physical Analyzer

(b)(4);(b)(7)(E)

Searching

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

Physical Analyzer

(b)(4),(b)(7)(E)

(b)(4);(b)(7)(E)

Find



(b)(4);(b)(7)(E)

(b)(4),(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4),(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4),(b)(7)(E)

Find



(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

Reporting

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4),(b)(7)(E)

(b)(4);(b)(7)(E)


(b)(4);(b)(7)(E)

Open (Advanced)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)



(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

Extraction

(b)(4);(b)(7)(E)



TCFTP UFED4PC



epic.org



EPIC-17-06-13-ICE-FOIA-20181115-Supplemental-Production-pt1

2018-ICLI-00030 1040



1

001040

My Celebrite

(b)(4);(b)(7)(E)

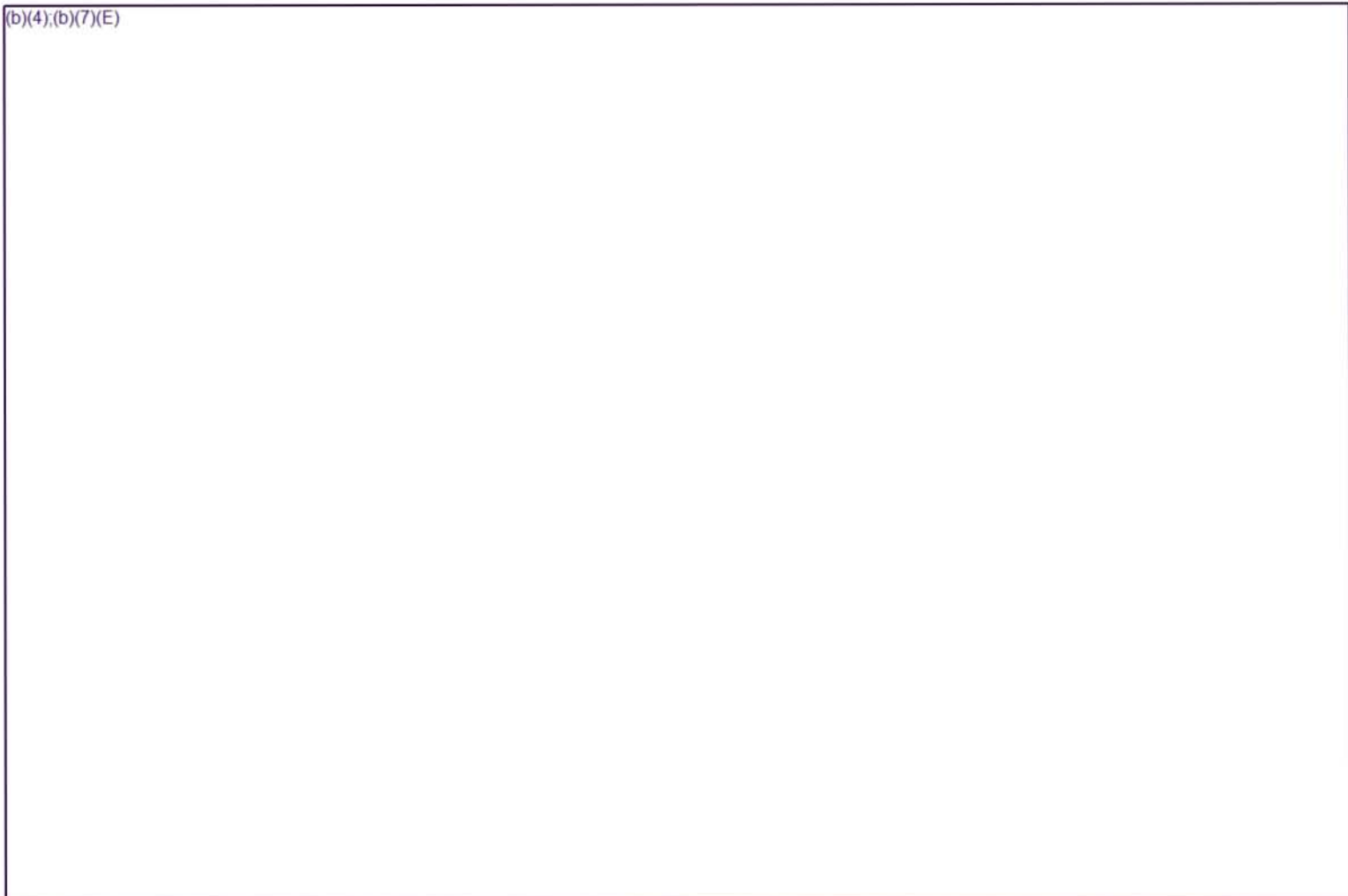
(b)(4);(b)(7)(E)

(b)(4),(b)(7)(E)

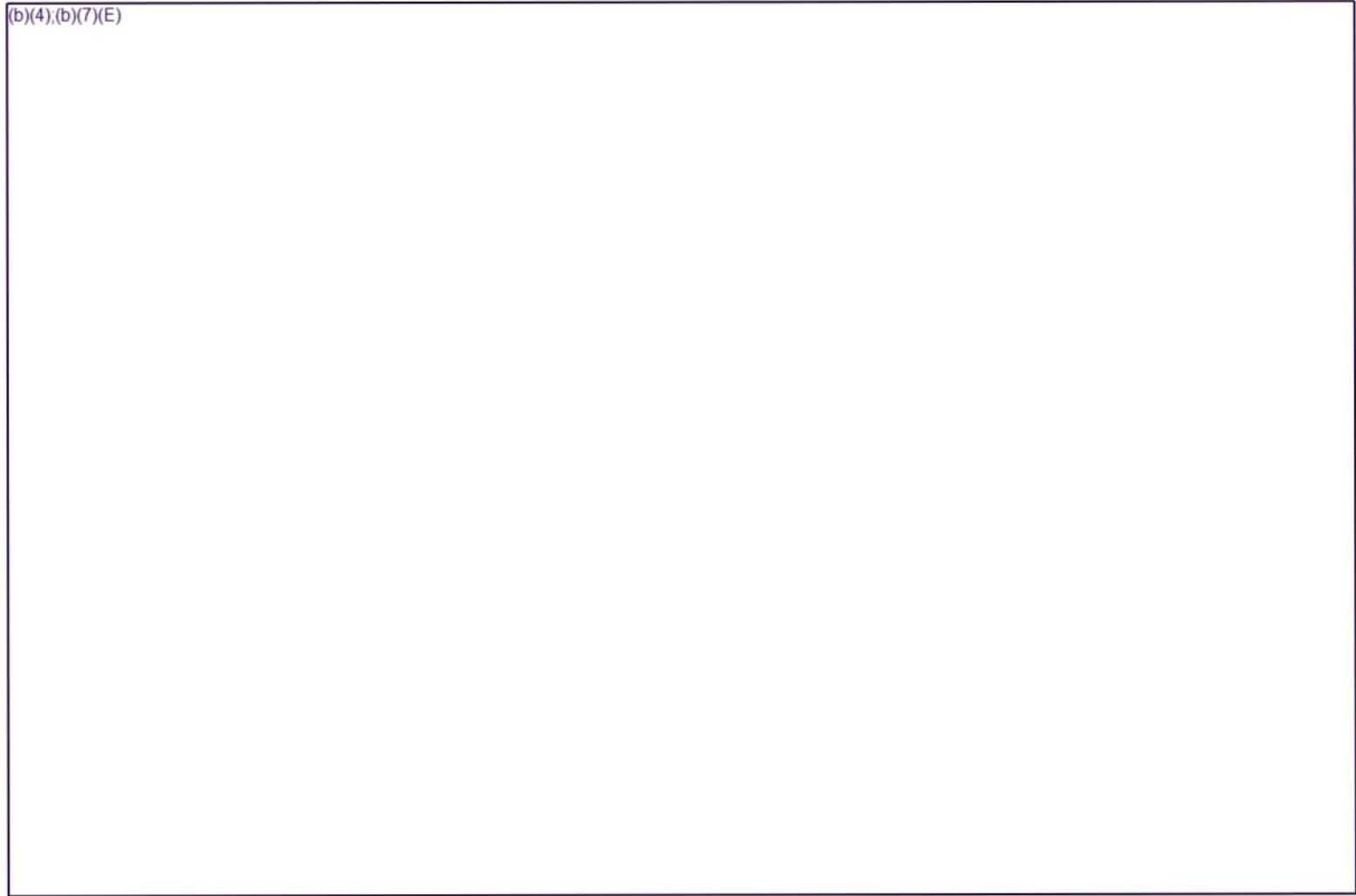
(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

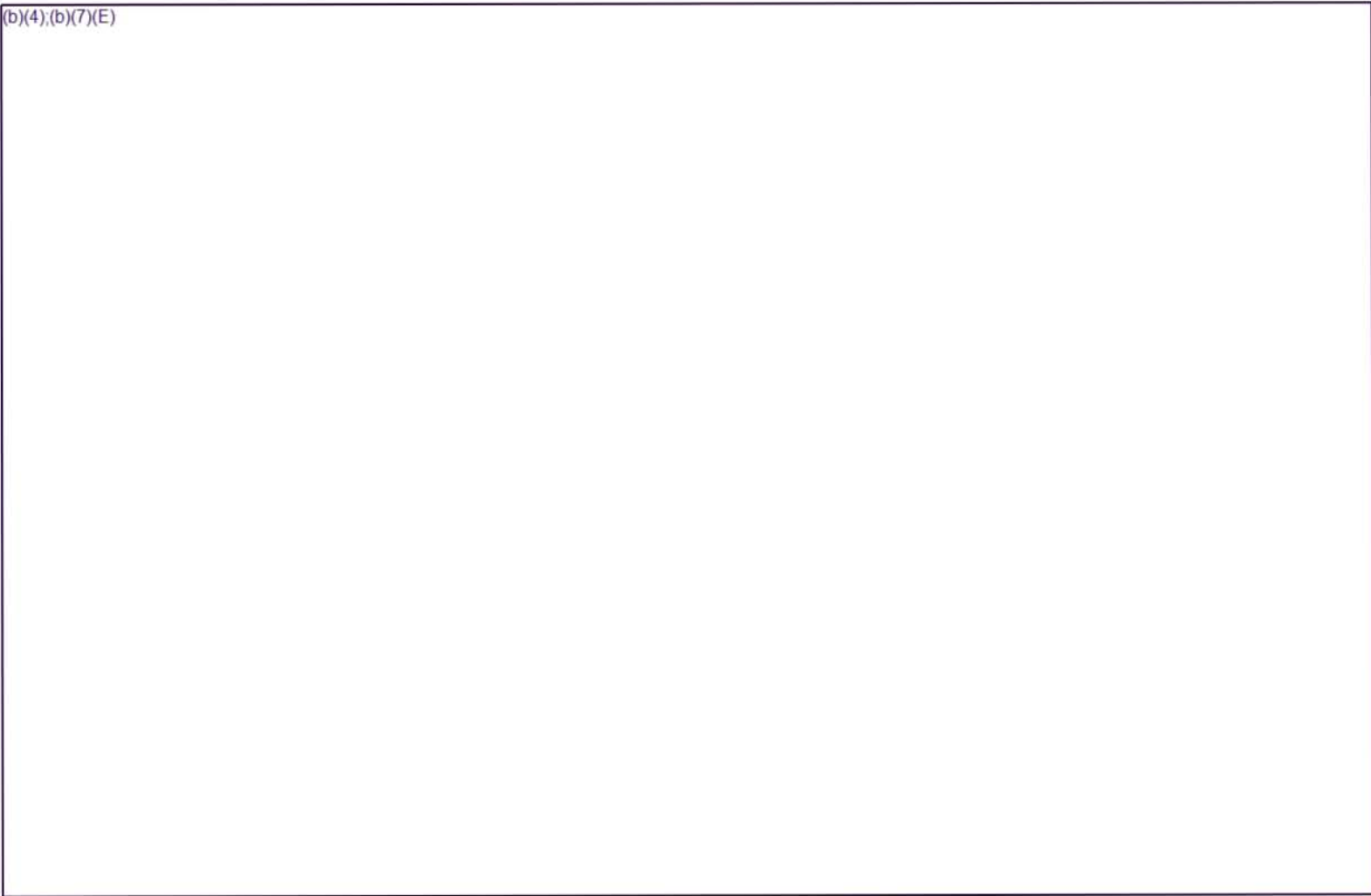
(b)(4);(b)(7)(E)



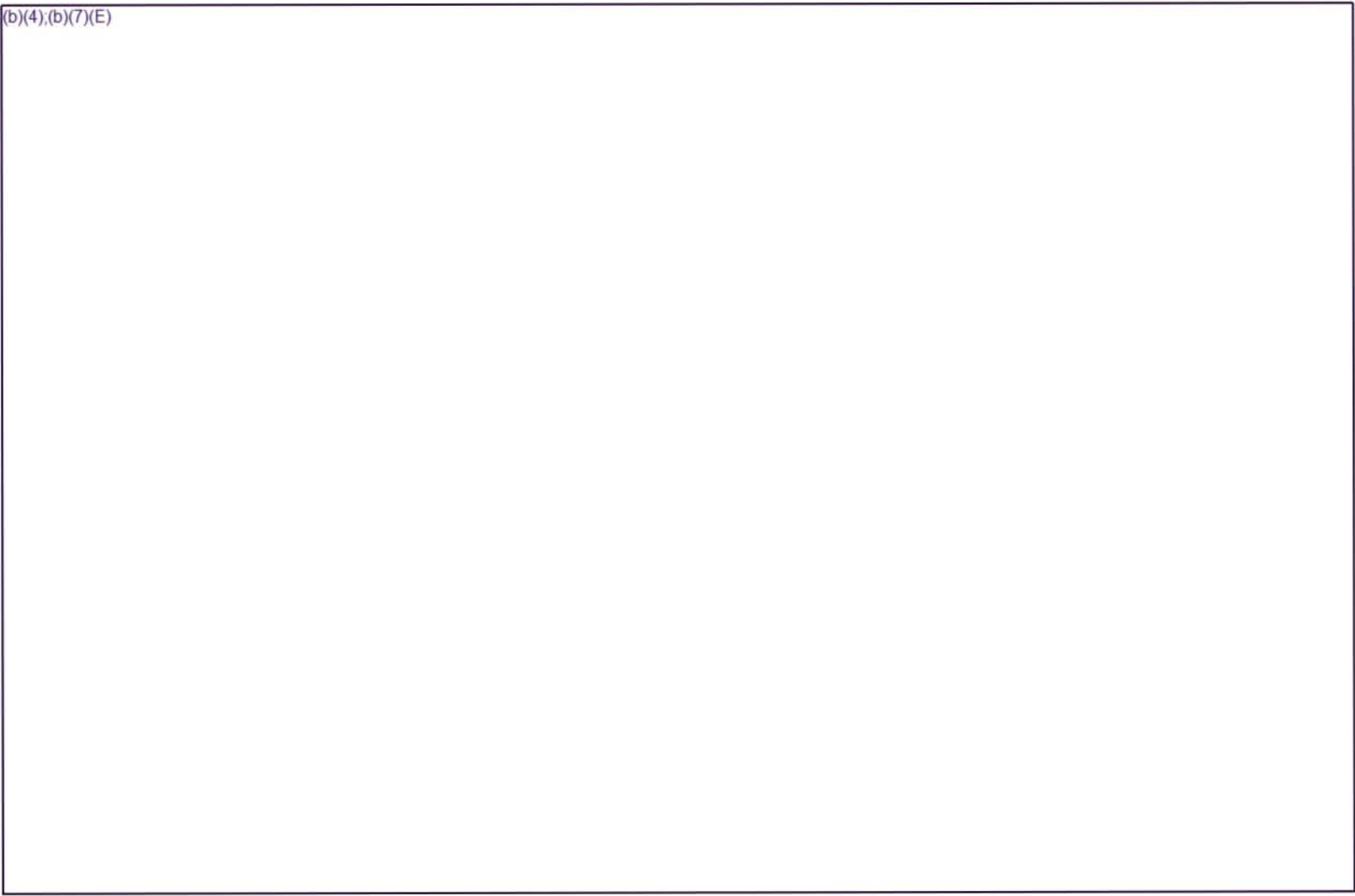
(b)(4),(b)(7)(E)



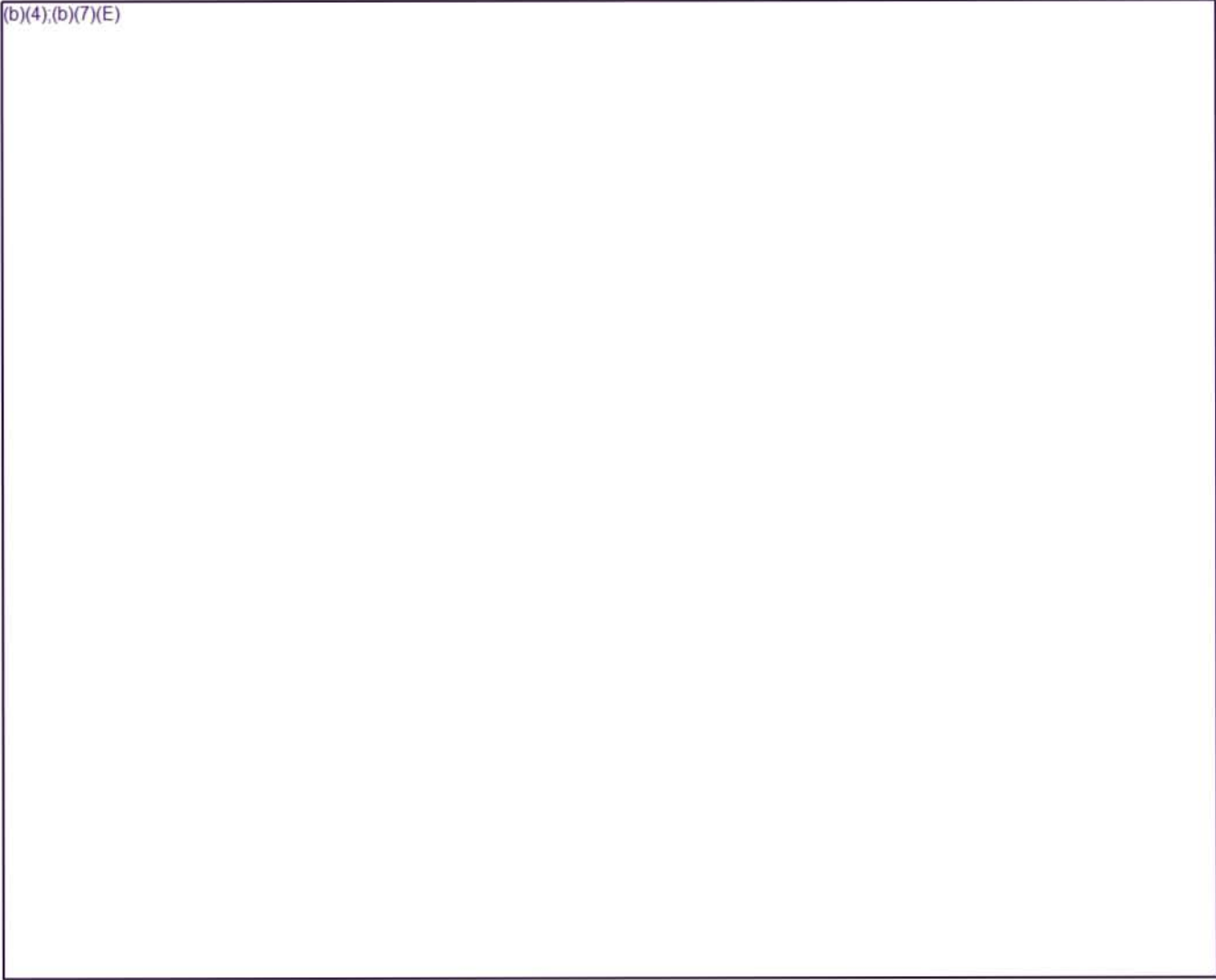
(b)(4);(b)(7)(E)



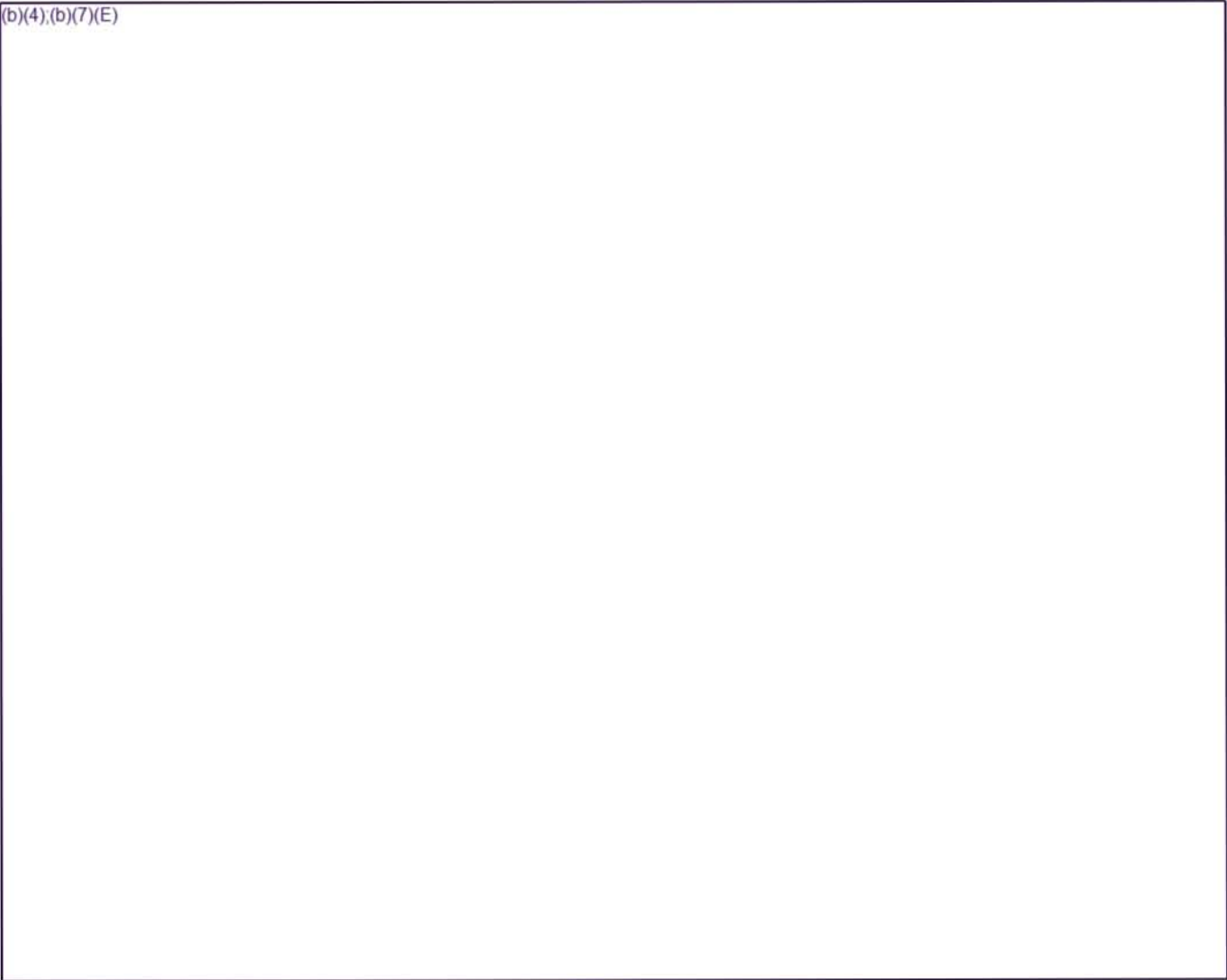
(b)(4),(b)(7)(E)



(b)(4);(b)(7)(E)



(b)(4),(b)(7)(E)



(b)(4);(b)(7)(E)

UFED4PC

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4),(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

TCFTP

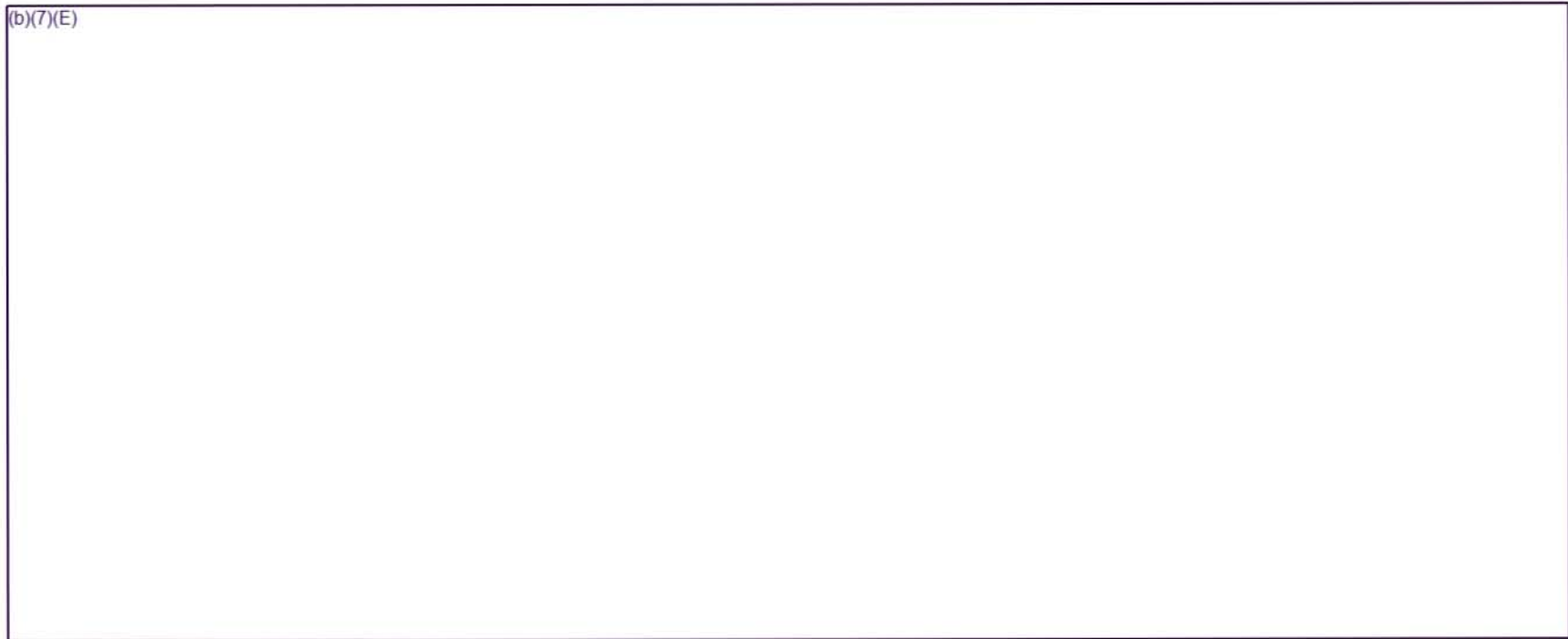
(b)(4);(b)(7)(E)

(b)(4),(b)(7)(E)

(b)(4);(b)(7)(E)

Auto Detection of Device iPhone Extraction

Cellebrite UFED4PC



(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

Cellebrite UFED4PC

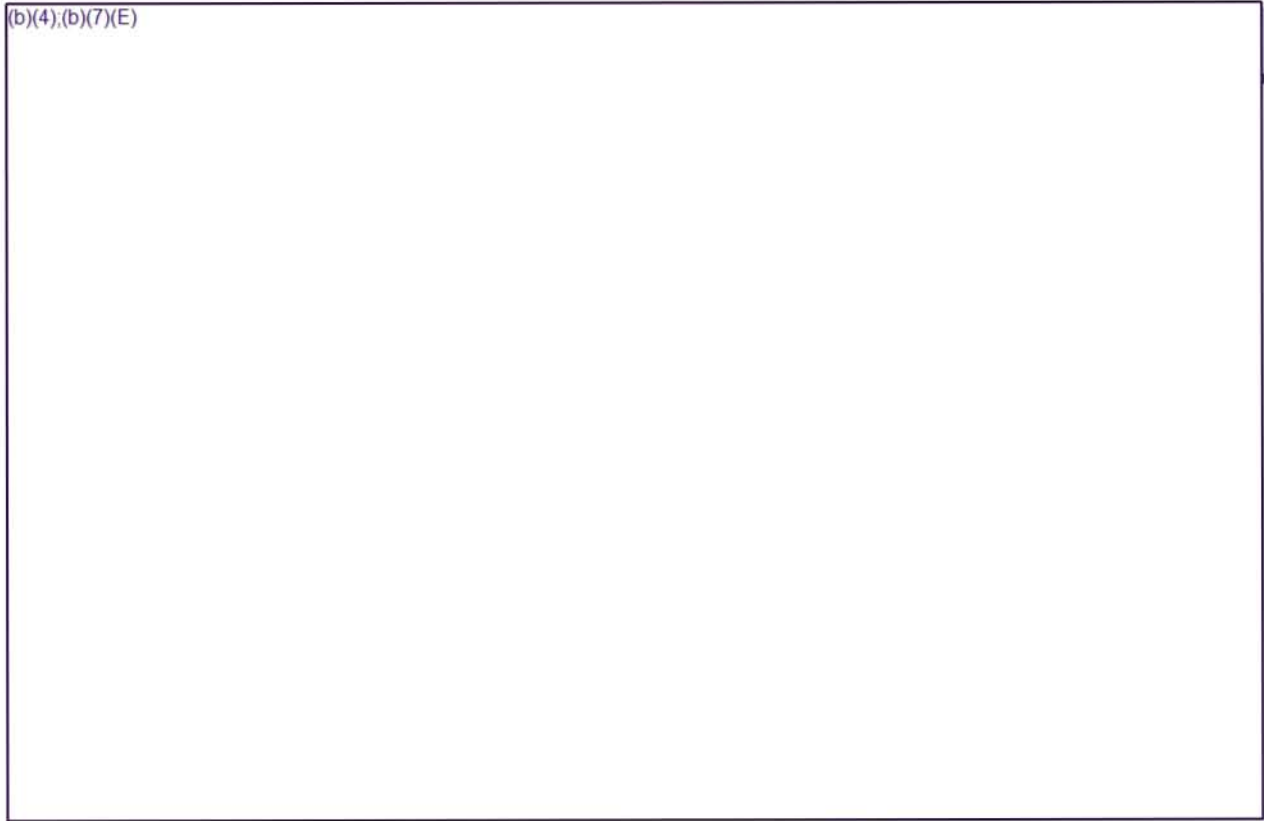
(b)(4),(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4),(b)(7)(E)

(b)(4),(b)(7)(E)

(b)(4);(b)(7)(E)



Manual Selection of Device Android Extraction

Cellebrite UFED4PC

(b)(4);(b)(7)(E)

Cellebrite UFED4PC

(b)(4);(b)(7)(E)

Cellebrite UFED4PC

(b)(4);(b)(7)(E)

Cellebrite UFED4PC

(b)(4),(b)(7)(E)

Cellebrite UFED4PC

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

Cellebrite UFED4PC

(b)(4);(b)(7)(E)

Cellebrite UFED4PC

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

Data Extraction

(b)(4);(b)(7)(E)

Cellebrite UFED4PC

(b)(4);(b)(7)(E)

Cellebrite UFED4PC

(b)(4);(b)(7)(E)

Cellebrite UFED4PC

(b)(4);(b)(7)(E)

Power Up Cable

Cellebrite Power Up Cable



The power up cable is used to power on cell phones if the battery is not present or malfunctions

Cellebrite Power Up Cable

- 1) Connect the Extra Power cable to the (b)(7)(E) in the back panel.
- 2) Connect the Data cable to the (b)(7)(E)
- 3) Identify the device's battery contacts:
 - Open the device's battery cover and remove the battery.
 - Locate the positive ('+') and negative ('-') pole markings, usually found next to the contacts area in the battery housing.
- 4) Connect the Red clip to the device's positive pole ('+'), the longer, primary Black clip to the negative pole ('-') and the shorter, secondary black clip between the two other clips, in adjacent to the primary Black clip. Make sure the clips are not closing a circuit by touching each other.

SIM Extraction

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

(b)(4),(b)(7)(E)

(b)(4);(b)(7)(E)

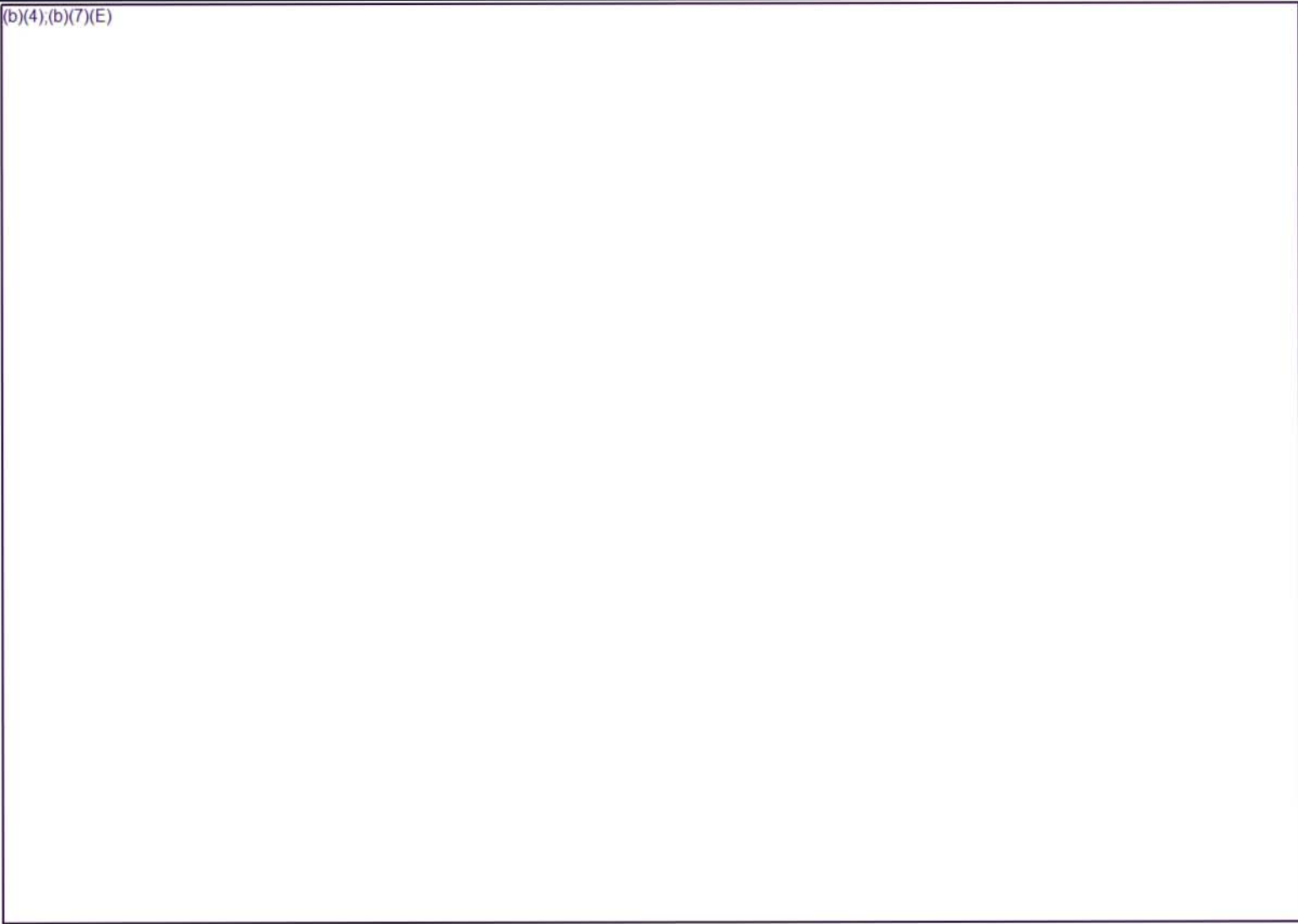
(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

SIM Cloning

(b)(4);(b)(7)(E)

(b)(4),(b)(7)(E)



(b)(4);(b)(7)(E)

(b)(4);(b)(7)(E)

