

**Bundesstrafgericht**

**Tribunal pénal fédéral**

**Tribunale penale federale**

**Tribunal penal federal**



\_\_\_\_\_  
Geschäftsnummer: BE.2009.6, BE.2009.7

**Entscheid vom 15. Februar 2010**  
**I. Beschwerdekammer**

\_\_\_\_\_  
Besetzung

Bundesstrafrichter Tito Ponti, Vorsitz,  
Emanuel Hochstrasser und Joséphine Contu,  
Gerichtsschreiber Stefan Graf

\_\_\_\_\_  
Parteien

**BUNDESANWALTSCHAFT,**

Gesuchstellerin

**gegen**

1. **A.**, vertreten durch Rechtsanwalt Markus Raess,

2. **B.**, vertreten durch Rechtsanwalt Bruno Steiner,

Gesuchsgegner

\_\_\_\_\_  
Gegenstand

Entsiegelung (Art. 69 Abs. 3 BStP)

**Sachverhalt:**

- A.** Die Bundesanwaltschaft führt gegen A. und B. sowie gegen weitere Beschuldigte ein gerichtspolizeiliches Ermittlungsverfahren, in dessen Rahmen sie am 6. und 8. März 2007 die privaten Räumlichkeiten der beiden Erstgenannten durchsuchen liess, wobei auf Einsprache der beiden Betroffenen hin die sichergestellten Dokumente und elektronischen Daten versiegelt wurden. Das daraufhin von der Bundesanwaltschaft gestellte (zu jenem Zeitpunkt zum Entscheid verbleibende) Entsiegelungsgesuch hiess die I. Beschwerdekammer mit Entscheid BE.2007.4 und BE.2007.5 vom 5. September 2008 teilweise gut und ermächtigte die Bundesanwaltschaft u. a. und im Sinne der Erwägungen, die verbleibenden Inhalte der sichergestellten Laufwerke nach Erfüllung der in E. 6.4 des Entscheides gemachten Auflage zu durchsuchen (Ziff. 3 des Dispositivs). Zudem auferlegte sie A. und B. die Gerichtsgebühr von Fr. 7'500.-- unter solidarischer Haftbarkeit zur Bezahlung (Ziff. 4 des Dispositivs). Das Bundesgericht hiess eine dagegen von der Bundesanwaltschaft erhobene Beschwerde teilweise gut und hob Dispositiv Ziffern 3 und 4 des angefochtenen bundesstrafgerichtlichen Entscheides auf. Es wies die I. Beschwerdekammer zudem an, die Triage (und nötigenfalls die Löschung) der fraglichen elektronischen Daten vorzunehmen und danach einen neuen Entscheid über die Zulässigkeit und den Umfang der Durchsuchung der sichergestellten Daten sowie über die Kosten des Entsiegelungsverfahrens zu fällen (Urteil des Bundesgerichts 1B\_274/2008 vom 27. Januar 2009). Dabei führte das Bundesgericht im erwähnten Urteil u. a. aus, der Entsiegelungsrichter könne bei der Triage zwar nötigenfalls – etwa zur Systematisierung und Sichtung grosser Datenmengen – geeignete technische Hilfsmittel, Experten und Hilfspersonen beiziehen, jedoch müsse die Triage und die allfällige Aussonderung von geheimnisgeschützten Daten im Entsiegelungsverfahren vom zuständigen Zwangsmassnahmengericht selbstverantwortlich wahrgenommen werden. Im Falle des Bezugs von spezialisierten Fachpersonen der Bundeskriminalpolizei sei hierbei besondere Sorgfalt darauf zu verwenden, dass diese keine unzulässige Einsicht in geheimnisgeschützte Daten erhielten (Urteil des Bundesgerichts 1B\_274/2008 vom 27. Januar 2009, E. 7).
- B.** In seiner Verfügung vom 27. Februar 2009 skizzierte der Präsident der I. Beschwerdekammer das mögliche weitere Vorgehen und lud die Parteien ein, sich hierzu zu äussern (act. 4). Aufgrund der eingegangenen Stellungnahmen (act. 5, 6 und 7) sowie aufgrund der technischen Hinweise der Bundeskriminalpolizei (act. 14) musste das beabsichtigte weitere Vorgehen betreffend die Durchsuchung der elektronischen Daten daraufhin modifi-

ziert werden. Der entsprechend angepasste modus operandi zur Durchsuehung der elektronischen Daten wurde den Parteien mittels Verfuegung des Praesidenten der I. Beschwerdekammer vom 26. Juni 2009 bekannt gegeben und die Bundeskriminalpolizei beauftragt, der I. Beschwerdekammer die Infrastruktur zur Durchsuehung der elektronischen Daten sowie weitere Unterstuetzungsleistungen zur Verfuegung zu stellen (act. 16). Zu Beginn des Monats September 2009 lagen der I. Beschwerdekammer die notwendigen technischen Mittel sowie die notwendigen Instruktionen von Seiten der Bundeskriminalpolizei schliesslich vor.

### **Die I. Beschwerdekammer zieht in Erwaeugung:**

1. Die I. Beschwerdekammer durchsuchte die vorliegenden elektronischen Daten mittels der Software ENCASE auf geheimnisgeschuetzte Inhalte (vgl. zu Inhalt und Umfang der geschuetzten Inhalte den Entscheid des Bundesstrafgerichts BE.2007.4 vom 23. Juli 2007, E. 4.4).
2. Bei der ersten Sichtung und Durchsuehung stellte sich heraus, dass verschiedene der Laufwerke, deren Inhalt von der Gesuchstellerin sichergestellt worden war, von den Gesuchsgegnern zur Datensicherung (sog. „backup“) verwendet worden waren, weshalb eine Vielzahl der sich auf den verschiedenen Laufwerken befindenden Computerdateien vollkommen identisch sind. Zur Erleichterung und Beschleunigung der Durchsuehung wurden deshalb saemtlichen Computerdateien sog. „hash values“ zugeordnet, was die systematische Auffindung und genaue Sortierung aller identischen Computerdateien ermoeglichte. Mit dieser Vorgehensweise konnte zwar vermieden werden, dass ueber dieselbe Computerdatei mehrfach entschieden werden musste; gleichzeitig machte sie aber die gemeinsame Durchsuehung einer jeweils spezifischen Auswahl (Filterfunktion nach Dateitypen) aus allen sichergestellten Computerdateien erforderlich.
3. Saemtliche sichergestellten Computerdateien sind in einem mittels ENCASE erstellten sog. „image“ enthalten, wobei der Inhalt des groessten Teils dieser Dateien auch mit Hilfe von ENCASE eingesehen werden kann. Im Hinblick auf die beabsichtigte Herausgabe aller nicht geheimnisgeschuetzten Daten an die Gesuchstellerin sind vorab saemtliche vorhandenen Computerdateien selektiert worden; eine Vielzahl von leeren Computerdateien (Groesse 0 KB) konnte hierbei nicht erfasst werden, was aber fuer die Strafverfolgungsbe-

hören insofern keinen Verlust bedeutet, als es sich bei den nicht erfassten ausnahmslos um Dateien ohne Inhalt handelt.

4. Im Anschluss daran wurden die bei der Durchsuchung identifizierten, geheimnisgeschützte Inhalte aufweisenden Computerdateien deselektiert.
  - 4.1 Diesbezüglich sind vorab sämtliche vorhandenen Textverarbeitungsdokumente (insgesamt 41'446 Computerdateien der Dateitypen „doc“, „pdf“, „wpd“, „rtf“ und „txt“) durchsucht worden. Dabei konnte festgestellt werden, dass die in Anhang I („doc“) und Anhang II („pdf“) aufgelisteten Computerdateien geheimnisgeschützte Inhalte aufweisen, weshalb sie im oben erwähnten Sinne deselektiert wurden.
  - 4.2 Anschliessend wurden sämtliche vorhandenen Maildateien (insgesamt 99'441 Computerdateien der Dateitypen „pst“, „ost“, „dbx“, „idx“, „mbx“, „eml“, „msg“ und „nsf“) mit Hilfe von ENCASE oder – nach vorgängiger Extraktion – mit anderen geeigneten Hilfsmitteln durchsucht bzw. gesichtet. Diesbezüglich war festzustellen, dass die in Anhang III („msg“) und Anhang IV („eml“) aufgelisteten Computerdateien geheimnisgeschützte Inhalte aufweisen, weshalb sie im oben erwähnten Sinne deselektiert wurden. Bei den acht vorhandenen Computerdateien des Dateityps „pst“ handelt es sich um komprimierte Mailarchive, welche eine Vielzahl einzelner E-Mailnachrichten beinhalten, die mit Hilfe von ENCASE jedoch nicht eingesehen werden können, weshalb sie zum jetzigen Zeitpunkt deselektiert wurden. Die Triage von deren Inhalt wird noch vorzunehmen sein und über deren Schicksal ist zu einem späteren Zeitpunkt zu entscheiden. Der Inhalt der einzigen vorhandenen Computerdatei des Dateityps „nsf“ konnte mit Hilfe von ENCASE ebenfalls nicht eingesehen werden, weshalb sie zum jetzigen Zeitpunkt deselektiert wurde. Die Triage von deren Inhalt wird noch vorzunehmen sein und über deren Schicksal ist ebenfalls zu einem späteren Zeitpunkt zu entscheiden.
  - 4.3 Die Durchsuchung sämtlicher sich auf den sichergestellten Laufwerken befindenden Bilddateien (insgesamt 277'554 Computerdateien der Dateitypen „art“, „bmp“, „gif“, „jpg“, „png“, „wmf“ und „tif“) ergab zwar, wie erwartet (act. 14), dass sich darunter vereinzelt auch eingescannte Dokumente befinden, dass jedoch keines davon geheimnisgeschützte Inhalte aufweist.
  - 4.4 Die Durchsuchung sämtlicher auf den sichergestellten Laufwerken vorhandenen Computerdateien des Dateityps „xls“ (mit Ausschluss derjenigen, die sich auf dem fast ausschliesslich Dateien dieses Typs beinhaltenden Laufwerk HD Lacie 150GB befinden und wofür die Gesuchsgegner ihre Ein-

sprache gegen die Durchsuchung bereits vorgängig zurückgezogen haben; BE.2007.4 und BE.2007.5, act. 47.3, 55 und 57) hat ergeben, dass der Gesuchsgegner 1 mit Hilfe dieses Dateityps verschiedentlich Faxmitteilungen erstellt hatte, dass jedoch keine dieser Mitteilungen geheimnisgeschützte Inhalte aufweist.

- 4.5** Die Durchsuchung der sich auf den sichergestellten Laufwerken befindenden Archivdateien des Dateityps „zip“ ist mit Hilfe von ENCASE nur unter Inkaufnahme erheblicher Geschwindigkeitseinbussen möglich, weshalb sie zum jetzigen Zeitpunkt ebenfalls deselektiert wurden. Die Triage von deren Inhalt wird noch vorzunehmen sein und über deren Schicksal ist zu einem späteren Zeitpunkt zu entscheiden.
- 4.6** Alle anderen sich auf den sichergestellten Laufwerken befindlichen Dateitypen weisen keine von den Gesuchsgegnern oder ihren Anwälten erstellte und demnach potenziell geheimnisgeschützte Inhalte auf, weshalb auf deren Durchsuchung durch die I. Beschwerdekammer verzichtet werden kann.
- 5.** Die I. Beschwerdekammer hat vom sog. „image“, welches alle sichergestellten Computerdateien beinhaltet, eine Kopie unter Ausschluss der erwähnten deselektierten (geheimnisgeschützte, leere oder noch zu durchsuchende) Computerdateien erstellt (vgl. E. 4), welche sie – nach Eintritt der Rechtskraft dieses Entscheides – der Gesuchstellerin auf einem externen Laufwerk zur Verfügung stellen wird. Bezüglich der vorerst deselektierten, aber noch zu durchsuchenden Computerdateien (Dateitypen „zip“, „nsf“ und „pst“) wird die I. Beschwerdekammer die Durchsuchung vornehmen und in einem weiteren Entscheid über deren Schicksal befinden, wobei das Verfahren diesbezüglich unter den Verfahrensnummern BE.2010.4 und BE.2010.5 weiterzuführen sein wird.
- 6.** Sämtliche Verfahrenskosten werden nach Abschluss aller Arbeiten bestimmt und verlegt.

**Demnach erkennt die I. Beschwerdekammer:**

1. Das Gesuch wird teilweise gutgeheissen und der Gesuchstellerin wird ein im Sinne der Erwägungen triagiertes „image“ auf einem externen Laufwerk zur Verfügung gestellt.
2. Über die vorerst deselektierten, von der I. Beschwerdekammer noch zu durchsuchenden Computerdateien (Dateitypen „zip“, „nsf“ und „pst“) wird in einem weiteren Entscheid befunden.

Das Verfahren wird diesbezüglich unter den Verfahrensnummern BE.2010.4 und BE.2010.5 weitergeführt.

3. Die Gerichtskosten werden nach Abschluss aller Arbeiten bestimmt und verlegt.

Bellinzona, 16. Februar 2010

Im Namen der I. Beschwerdekammer  
des Bundesstrafgerichts

Der Präsident:

Der Gerichtsschreiber:

i.V. Emanuel Hochstrasser,  
Bundesstrafrichter

**Zustellung an**

- Bundesanwaltschaft
- Rechtsanwalt Markus Raess
- Rechtsanwalt Bruno Steiner

**Beilagen**

Anhang I bis IV als pdf-Dateien auf CD-ROM

**Rechtsmittelbelehrung**

Gegen Entscheide der I. Beschwerdekammer über Zwangsmassnahmen kann innert 30 Tagen nach der Eröffnung der vollständigen Ausfertigung beim Bundesgericht Beschwerde geführt werden (Art. 79 und 100 Abs. 1 des Bundesgesetzes über das Bundesgericht vom 17. Juni 2005; BGG). Das Verfahren richtet sich nach den Artikeln 90 ff. BGG.

Eine Beschwerde hemmt den Vollzug des angefochtenen Entscheides nur, wenn der Instruktionsrichter oder die Instruktionsrichterin es anordnet (Art. 103 BGG).