

Case Report

National Gallery DC

Tracy's iPhone [2012-07-15-National-Gallery]

Table of Contents

[Case Report](#)

[National Gallery DC](#)

[Tracy's iPhone \[2012-07-15-National-Gallery\]](#)

[Table of Contents](#)

[Executive Summary](#)

[Equipment and Tools](#)

[Details of Tracy's iPhone](#)

[Evidence to Establish Personas](#)

[Evidence relating to theft of valuable stamps](#)

[Evidence relating to defacement of museum art](#)

[Plot Timeline](#)

[Conclusion](#)

[Appendix A: Correspondence Evidence](#)

[Appendix B: Wi-Fi and GPS Location Information](#)

Executive Summary

On January 21, 2016, Digitech Inc. called in to assist the National Gallery, Washington D.C. (NGDC) case involving the conspiracy associated with the theft of valuable stamps and defacing of museums are at the NGDC.

- Tracy is a suspect in the mentioned conspiracy.
- As part of the investigation, Tracy's iPhone was taken into custody.
- Digitech, Inc. was tasked with investigating evidence relevant to the conspiracy.

As described fully in the report, Digitech, Inc. made the following findings.

Equipment and Tools

Tool(s)	Equipment	Description
Kali Linux 4.18.0	Machine	Linux is an operating system.
Autopsy 4.10.0	Software	Digital forensics investigation use Autopsy in Kali Linux
Nano	Software	Terminal base text editor
SQLitebrowser	Software	Is an embedded relational database engine.
Azure – Remote Desktop	Software	App virtualization server that runs on the cloud and access on my remote Desktop anytime.

Details of Tracy's iPhone

Name	Findings	Location in iPhone image file
Model	iPhone 1,2	/mobile/Library/Logs/AppleSupport/general.log
Host Name	Tracy Sumtweleve's iPhone	/logs/lockdownd.log
OS Version	iPhone OS 4.2.1 (8C148)	/mobile/Library/Logs/AppleSupport/general.log
Install Time	6/6/2012 12:03:28	/logs/lockdownd.log

User Email	tracysumtwelve@gmail.com , coralbluetwo@hotmail.com tracysumtwelve@nationalgallerydc.org	/vol5/mobile/Library/Mail/Envelope Index
Phone Number	(703) 340-9661	/logs/lockdownd.log
Serial Number	86004482Y7H	/logs/AppleSupport/general.log
ICCID	890141032551953423366	/logs/lockdownd.log
IMEI	012021003735398	/root/Library/lockdown/activation_records/wildcat_record_plis
MD5 Hash	34c4888f095dc3241330462923f6fea5	/root/corpus/tracy.orginal.md5.log.txt
SHA256 Hash	71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607	/root/corpus/tracy.orginal.sha256.log.txt

Evidence to Establish Personas

This section establishes aliases, phone numbers, emails addresses associated with each person, and relationships between each individual.

Tracy:

Phone Number: (703) 340-9961
 Personal Email: tracysumtwelve@gmail.com, coralbluetwo@hotmail.com
 Work Email: tracy.sumtwelve@nationalgallerydc.org
 Relationship: Accused

Pat:

Phone Number: (571) 308-3236
 Email: perrypatsum@yahoo.com
 Relationship: Tracy's brother

Terry:

Phone Number: (703) 829-6071

Email:

Relationship: Tracy's daughter

Joe:

Phone Number:

Email: joe.sum.twelve@gmail.com

Relationship: Tracy's ex-husband

Carry:

Phone Number: (202) 725-2124

Email: carrysum2012@yahoo.com

Relationship: friend

Suspect:

Email: King Kthings throne1966@hotmail.com

Evidence relating to theft of valuable stamps

This sub-section provides details regarding the evidence found as it relates to the theft of valuable stamps.

Tracy has been having an ongoing dialog with her brother about stealing specific items (Stamps) from the National Gallery. I suspected the Tracy and Pat plans to sending emails each other and secret.

Evidence relating to defacement of museum art

This sub-section provides details regarding the evidence found as it relates to the defacement of museum art.

Carry organized a Flash Mob at the gallery. Carry tried developing the plan to break them into the museum with the tools they need to damage the artwork. Carry used a tablet computer and sets it up to use her catumtwelve email account dealings with Alex setting up the flash mob. Carry is interested in security, schedules, events, and locations where art will be displayed. She watched to keep them and plans break-in at the Gallery. Carry communicate with Alex, Tracy, Pat, and Robbers.

Plot Timeline

Name	Timeline
Pat	Fri Jul 06 2012 15:02:19
Pat	Fri Jul 06 2012 15:02:19
Pat	Fri Jul 06 2012 15:11:54
Pat	Fri Jul 06 2012 15:13:31
Carry	Fri Jul 06 2012 16:27:16
Carry	Fri Jul 06 2012 16:27:50
Terry	Fri Jul 13 2012 01:02:10
Fraud from Scam	Sat Jul 07 2012 19:36:35
Carry	Thu Jul 05 2012 18:18:23
Carry	Thu Jul 05 2012 18:20:26
Carry	Thu Jul 12 2012 17:06:45
Terry	Tue Jul 03 2012 13:41:51
Terry	Tue Jul 03 2012 14:04:32
Pat	Tue Jul 10 2012 15:26:19
Pat	Tue Jul 10 2012 15:58:04
Terry	Tue Jul 10 2012 17:18:38
Terry	Tue Jul 10 2012 18:19:24
Terry	Tue Jul 10 2012 18:58:24
Pat	Tue Jun 12 2012 21:25:04
Carry	Wed Jul 11 2012 12:41:45
Carry	Wed Jul 11 2012 12:49:08
Terry	Wed Jun 13 2012 17:30:28
Pat	Wed Jun 13 2012 18:30:38
Terry	Wed Jun 13 2012 18:33:46

Mon 9
July
2012
10:44:1
1

From: Tracy Sumtweleve
tracysumtweleve@gmail.c
om To:
coralbluetwo@hotmail.co
m

Subject: Things Attachment: documents.zip

Tues
19 June
2012
14:38:5
9

From:
perryatsum@yahoo.com
To:
coralbluetwo@hotmail.co
m

Subject: Crazydave by the VMS Hey Coral Just got your email.
That took longer than expected! Oh well! You've got to check
out this new song by the VMs. I love the base. Tell me what
you think!

Tues
10 July
2021 at

Forward message- From:
King Kthings
throne1966@hotmail.com

Subject: RE: can't pass up You're too kind... I got you brotha.
I need some tools in order ot do this job for you. Here are
some requirements that I will need: See attachment

11:19 AM To: patsumtwelve@gmail.com
From: Pat
Tues TeeSumTweleve
10 Jul patsumtwelve@gmail.com
2012 To:
11:24:5 coralbluetwo@hotmail.co
7 m

Subject: Fwd: can't pass up this is what we need to get for the guy that's going to make our job happen 9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx

From: patsumtwelve@gmail.com
Tues To:
10 Jul thron1966@hotmail.com
2012 Cc:
11:24:5 coralbluetwo@hotmail.co
8 m

King, Long time no see... I have a juicy proposition for you. Two weeks from now, me and my associates are planning a heist at the national gallery. Although, we need a helping hand. I know that you are on parole right now and are probably hesitant to participate. Me and your parole office go years back. He is a very strict fellow. If he were to find out that you were dealing drugs and shooting dope in your veins every night, I feel he wouldn't be too happy. Its very easy for a person to phone the feds an anonymous tip that you are on drugs and the location of your stash. All they have to do is give you a drug test and since you're on parole, the feds don't need a search warrant. Well hit me up you where to find me. Attachment filename = "needs.txt"

Conclusion

Evidence found on Tracy's iPhone indicated the following:

The suspect King Kthings came from robbers because robbers wrote to Pat and called "I got you Brotha included attachment file needs.txt from email. Then Pat sent two emails to Tracy tracysumtwelve@gmail.com, coralbluetwo@hotmail.com with attachment file needs. Txt. Pat texted to Tracy to explain a email the attachment change to convert to pdf. The needs.pdf opened what they need lists things. Needs lists: A rope and javelin (using alternative means to break in) -tactical turtlenecks (what i will be wearing) -spray paint (for the cameras) - vibram five finger shoes (in order to walk silently) -pack of smokes (detecting lasers) - smoke grenades (use as a means of escape if caught

Appendix A: Correspondence Evidence

This subsection will provide an amalgamation of the email and SMS correspondence evidence.

Email:

Artifact #	Name of File:	Key Information Y/N
1.	01FE9965-A923-40CF-A78A-72CE3BD26571.emlx	N

2.	3896FC6F-A083-4D39-B0A2-CE68368D44CA.emlx	N
3.	8A3BD06F-CDB1-4453-9C69-77E06823F2AE.emlx	Y
4.	9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx	Y
5.	F3F4EB95-52EB-42FC-9279-46DAB24B6E34.emlx	N

Master Timeline of NGDC				
Artifact #	Timestamp	Header Information	Key Information	Evidence Location
1.	Tues, 19 June 2012 14:38:59	From: perryatsum@yahoo.com To: coralbluetwo@hotmail.com Subject: Crazydave by the VMS	Hey Coral, Just got your email. That took longer than expected! Oh well! You've got to check out this new song by the VMs. I love the base. Tell me what you think!	Mailbox Data Structure -
2.	Mon, 9 July 2012 10:44:11	From: Tracy Sumtweleve tracysumtweleve@gmail.com To: coralbluetwo@hotmail.com Subject: Things	Attachment: documents.zip	8A3BD06F-CDB1-4453-9C69-77E06823F2AE.emlx
3.	Tues 10, Jul 2012 11:24:57	From: Pat TeeSumTweleve patsumtweleve@gmail.com To: coralbluetwo@hotmail.com Subject: Fwd: can't pass up	this is what we need to get for the guy that's going to make our job happen	9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx
4.	Tues 10, July 2021 at 11:19	Forward message- From: King Kthings	You're too kind... I got you brotha. I need some	9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx

	AM	throne1966@hotmail.com To: patsumtwelve@gmail.com Subject: RE: can't pass up	tools in order ot do this job for you. Here are some requirements that I will need: See attachment	
5.	Fri 6 July 2012 11:49:31	From: patsumtwelve@gmail.com To: thron1966@hotmail.com Cc: coralbluetwo@hotmail.com	King, Long time no see... I have a juicy proposition for you. Two weeks from now, me and my associates are planning a heist at the national gallery. Although, we need a helping hand. I know that you are on parole right now and are probably hesitant to participate. Me and your parole office go years back. He is a very strict fellow. If he were to find out that you were dealing drugs and shooting dope in your veins every night, I feel he wouldn't	9F0508B8-04FB- 490E-A7F0- 3E23B0E7C59B.emlx

			<p>be too happy. Its very easy for a person to phone the feds an anonymous tip that you are on drugs and the location of your stash. All they have to do is give you a drug test and since you're on parole, the feds don't need a search warrant. Well hit me up you where to find me.</p> <p>Attachment filename = "needs.txt"</p>	


SMS is here:





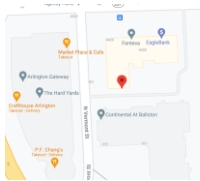
Relation /Friend	Ph1	Ph2	Text
	1571	1339	
Tracy's brother	3083	5363	
	236	04	What are you up to this weekend? 2 0 3 0 0 4 0 us 1
Tracy's daughter	1703	1339	
	8296	6086	I'm going out with dad after school for pizza! Thought I'd let you know if you planned to cook.
	071	28	
	1571	1339	
Tracy's brother	3083	6122	
	236	38	I don't have any big plans. How about you? 3 0 3 0 0 4 0 us 1
Tracy's daughter	1703	1339	
	8296	6124	
	071	26	Ok, sounds good. 3 0 4 0 0 4 0 us 1






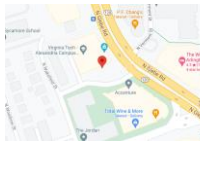
Tracy's daughter	1703 071	1341 11	Hey honey. I'm not sure if we can afford Prufrock anymore... What do you think about maybe switching to someplace else? 3 0 4 0 0 4 0 us 1
Tracy's daughter	1703 8296 071	1341 3242 72	moving schools at this point would be the worst! i would rather live with dad and stay at prufrock then change schools :(2 0 4 0 0 4 0 us 1
Tracy's Friend - Carry	1202 7252 124	1341 5123 03	Sounds good let's shoot for one àt Bubba s grill 2 0 5 0 0 4 0 us 1
Tracy's Friend - Carry	1202 7252 124	1341 5124 26	Okay that sounds great. See you there 3 0 5 0 0 4 0 us 1
Tracy's brother	1571 3083 236	1341 5869 39	Hey can you give me a call 3 0 3 0 0 4 0 us 1
Tracy's brother	1571 3083 236	1341 5873 17	Sis I'm really busy can we can do this later 2 0 3 0 0 4 0 us 1
Tracy's brother	1571 3083 236	1341 5875 14	pat this is important I need you to call me soon 3 0 3 0 0 4 0 us 1
Tracy's brother	1571 3083 236	1341 5876 11	Ok I'll call in 5 2 0 3 0 0 4 0 us 1
Tracy's Friend - Carry	1202 7252 124	1341 5920 36	I have a table inside 2 0 5 0 0 4 0 us 1
Tracy's Friend - Carry	1202 7252 124	1341 5920 70	Okay brt 3 0 5 0 0 4 0 us 1
Fraud from Scam	1206 9100 932	1341 6897 95	Congratulations, your entry in last months drawing won you a FREE \$1,000 Target Giftcard! Enter "703" at www.target.com.trdt.biz to tell us where to ship it 2 0 6 0 0 0 0 us 1
Tracy's brother	1571 3083 236	1341 9339 79	hey sis yo friend coral got a email the attachment needs to be changed to pdf let her know 2 0 3 0 0 4 0 us 1
Tracy's brother	1571 3083 236	1341 9358 84	Sure thing I'll get on it 3 0 3 0 0 4 0 us 0 1341938229 33 0 3 0 0 0 0 us 0
Tracy's daughter	1703 8296 071	1341 9407 18	Going to lunch. You want to go????! 3 0 4 0 0 4 0 us 1
Tracy's daughter	1703 8296 071	1341 9443 64	Back at work 3 0 4 0 0 0 0 us 1
Tracy's daughter	1703 8296 071	1341 9467 04	I'm busy. Maybe this weekend if dad isn't busy 2 0 4 0 0 0 0 us 1




Tracy's	1202	1342	
Friend -	7252	0105	
Carry	124	05	I'm almost there where should I meet you? 2 0 5 0 0 4 0 us 1
Tracy's	1202	1342	
Friend -	7252	0109	
Carry	124	48	Just meet me out front, I'll take the tablet in. 3 0 5 0 0 4 0 us 0
Tracy's	1202	1342	
Friend -	7252	1128	
Carry	124	05	How's the flashmob going 3 0 5 0 0 0 0 us 0
Tracy's	1703	1342	
daughter	8296	1413	I really want to go to Dad's this weekend. He said he'll take me shopping for school 0 0 4 0 0 0 0 us 0
r	071	30	

Appendix B: WiFi and GPS Location Information

Location Information				
Artifact #	Timestamp	Header Information	Body	Map Screenshot
1. MAC 44:1e:a1:f4:d: 7f	3.6130688247371 5E8	38.88055896 - 77.11553561	900 N Glebe Rd, Arlington, VA	

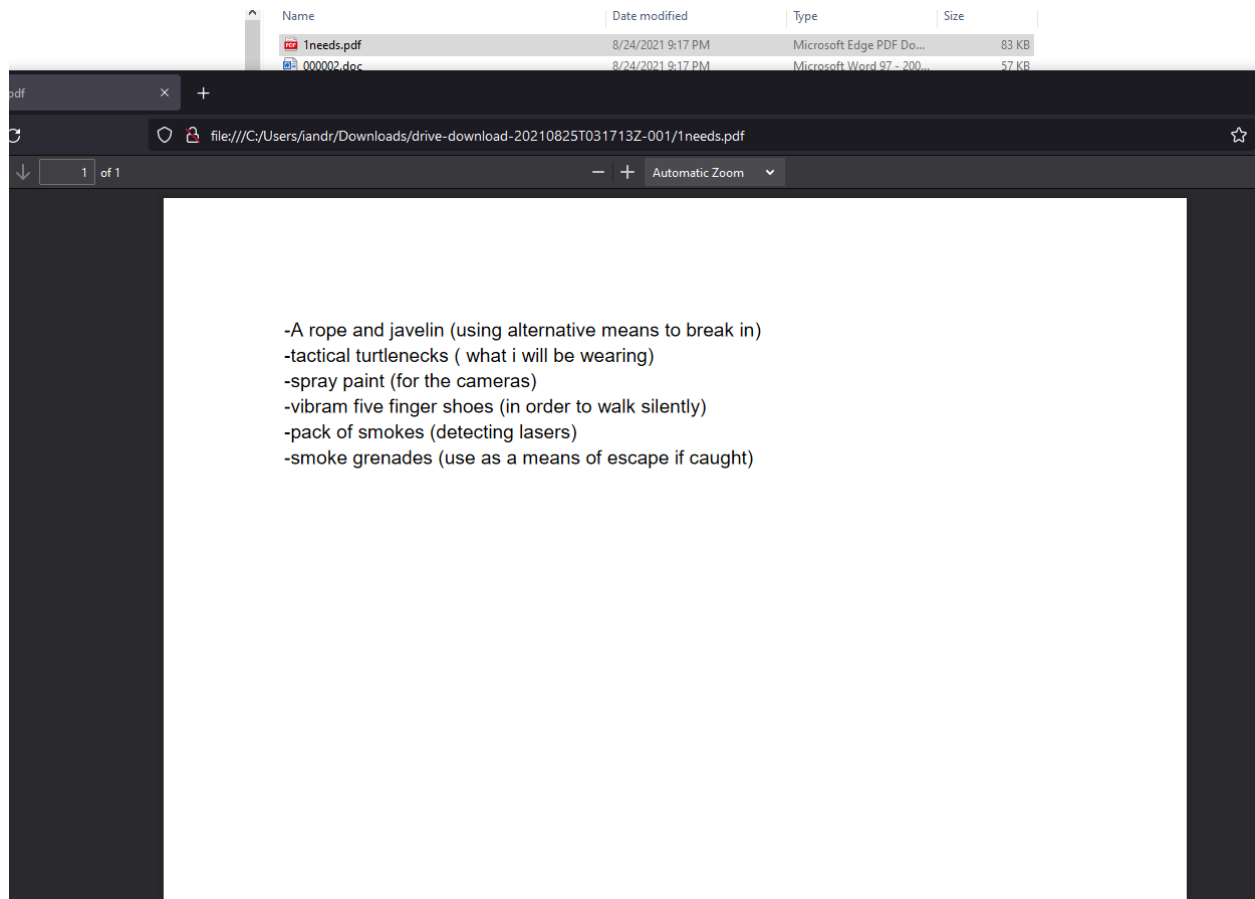
			22203	
2. MAC 0:26:b8:ac:1c:10	3.61306882473715E8	38.88005346 - 77.11595332	801 N Wakefield St, Arlington, VA 22203	
3. c0:c1:c0:15:66:fa	3.61306882473715E8	38.88093715 -77.11640596	Bluemont, Arlington, VA 22203	
4. e0:46:9a:3f:1b:a6	3.61306882473715E8	38.87996816 -77.11601394	801 N Wakefield St, Arlington, VA 22203	
5. e4:e0:c5:f:29:fa	3.61306882473715E8	38.88143724 -77.11478394	851 N Glebe Rd, Arlington, VA 22203	
6. 0:18:1:fb:b2:c3	3.61306882473715E8	38.8815732 -77.11455619	4420 Fairfax Dr, Arlington, VA 22203	

7. 10:9a:dd:83:92:13	3.61306882473715E8	38.88141357 -77.11484962	901 N Glebe Rd, Arlington, VA 22203	
8. 0:1f:90:e8:ff:42	3.61306882473715E8	38.88152045 -77.11477804	901 N Vermont St, Arlington, VA 22201	
9. 0:1f:90:ed:3c:2e	3.61306882473715E8	38.88144159 -77.1140722	851 N Glebe Rd UNIT 202, Arlington, VA 22203	
10. 68:7f:74:94:aa:ed	3.61306882473715E8	38.88133615 -77.11399537	900 N Taylor St, Arlington, VA 22203	
11. 0:1f:90:fd:9:60	3.61306882473715E8	38.88140815 -77.1137892	Virginia Square, Arlington, VA 22203	
12. 0:24:6c:67:e9:20	3.61306882473715E8	38.88062763 -77.11558109	900 N Glebe Rd, Arlington, VA 22203	

13. 0:24:6c:67:d9:60	3.61306882473715E8	38.8806498 -77.11627441	841 N Wakefield St, Arlington, VA 22203	
1.4 0:26:62:d8:b4:20	3.61306882473715E8	38.8797456 -77.11526322	4501-4507 Wilson Blvd, Arlington, VA 22203	
15. 58:6d:8f:f8:29:3c	3.61306882473715E8	38.8807792 -77.11643189	837 N Wakefield St, Arlington, VA 22203	

I found some files from Tracy's email attachment files. But I opened the needs.txt file part hide complex but noticed a comment with pdf issue. So I copied to pasted from needs.txt to 1needs.txt, then rename this file with .pdf.

Here's evidence 1needs.pdf



Here are the files about insurances.



NATIONAL GALLERY DC
WASHINGTON



Memorandum of Insurance Assurance:

TO: MylStamp Collections

In Regards to items owned or on loan to the National Gallery DC , Washington from MylStamp Collections from the period of May 12, 2012 to May 12, 2013, all items in aforementioned list will be in the custody of National Gallery DC and therefore fiscal responsibility of said items is carried by the same. As per agreement between both parties the following items are covered by AwesomeInsurance Inc. Policy x23654 for the following amounts under any circumstances leading to the degradation of said items excepting normal wear of display.

Lot # 25. Armed Forces Reserve	\$43,000.00
Lot # 26. Stamp of Kazakstan2	\$29,000.00
Lot# 27. BradyCo.	\$12,000.00

Terms do not cover period of transport from or to the National Gallery.

D'Mann

President National Gallery DC

For The Internal use of National Gallery and MylStamp Collections Only.



NATIONAL GALLERY DC
WASHINGTON



Memorandum of Insurance Assurance:

TO: MylStamp Collections

In Regards to items owned or on loan to the National Gallery DC , Washington from MylStamp Collections from the period of May 12, 2012 to May 12, 2013, all items in aforementioned list will be in the custody of National Gallery DC and therefore fiscal responsibility of said items is carried by the same. As per agreement between both parties the following items are covered by AwesomeInsurance Inc. Policy x23654 for the following amounts under any circumstances leading to the degradation of said items excepting normal wear of display.

Lot # 11. Woman's Profile	\$31,000.00
Lot # 12. Stamp of Kazakhstan	\$29,000.00
Lot# 13. 1929 Nepal	\$27,000.00

Terms do not cover period of transport from or to the National Gallery.

D'Mann

President National Gallery DC



NATIONAL GALLERY DC
WASHINGTON



Memorandum of Insurance Assurance:

TO: MylStamp Collections

In Regards to items owned or on loan to the National Gallery of Art, Washington from MylStamp Collections from the period of May 12, 2012 to May 12, 2013, all items in aforementioned list will be in the custody of National Gallery DC and therefore fiscal responsibility of said items is carried by the same. As per agreement between both parties the following items are covered by AwesomeInsurance Inc. Policy x23654 for the following amounts under any circumstances leading to the degradation of said items excepting normal wear of display.

Lot # 1. Douglas MacArther	\$35,000.00
Lot # 2. Nederland	\$30,000.00
Lot# 3. Mongolia	\$24,000.00

Terms do not cover period of transport from or to the National Gallery.

D'Mann

President National Gallery DC

For The Internal use of National Gallery and MylStamp Collections Only.



STATEMENT

United States Department of Agriculture • Office of Communications • 1400 Independence Avenue, SW
Washington, DC 20250-1300 • Voice: (202) 720-4623 • Email: oc.news@usda.gov • Web: <http://www.usda.gov>

Release No. 0043.04
Office of Communications (202) 720-4623

BSE Update – January 27, 2004

Depopulation Activities

On Monday, Jan. 26, 2004, 18 animals of interest were euthanized and sampled from the Quincy, WA, facility. Four animals of interest were euthanized and sampled at the Tenino, WA, facility. In addition to these two facilities, USDA has previously conducted selective depopulation activities at these facilities:

- Bull calf premises - a total of 449 animals depopulated
- Mabton, WA (index premises) - a total of 131 animals depopulated
- Mattawa, WA - a total of 39 animals depopulated
- Connell, WA - a total of 15 animals depopulated
- Boardman, OR - a total of 20 animals depopulated

To date, all 170 samples from the index herd and the Mattawa herd have completed testing; results were negative for BSE. The final test results for the samples taken at Connell, WA; Boardman, OR; Quincy, WA; and Tenino, WA are not yet available.

Investigation Activities

At this time, 28 of the 81 animals that came from Canada have been located:

- 1 of the 81 is the BSE-positive cow and was located in the Index herd in Mabton, Washington.
- 9 of the 81 were located in the Index herd in Mabton, Washington.
- 3 were located at a facility in Tenino, Washington.
- 6 were located at a facility in Connell, Washington.
- 1 was located at a facility in Quincy, Washington.
- 3 were located at a facility in Mattawa, Washington.
- 1 is located at a facility in Moxee, Washington.
- 3 are located at a facility in Burley, Idaho.
- 1 is located at a facility in Othello, Washington.

Guidelines on bovine spongiform encephalopathy (BSE) issued by the World Organization for Animal Health (OIE), the international animal health standard setting organization, state that animals born on a premises within one year (before or after) of a BSE-affected animal can be considered of significant interest to the country reporting the

BSE detection. As such, USDA is focusing on 25 of the 81 animals also born into the birth herd of the index animal. Based on normal culling practices of local dairies, USDA's Animal and Plant Health Inspection Service estimated that the Agency would be able to locate approximately 11 of these animals. APHIS has definitively located 14 of these animals.

USDA has also been investigating 17 additional cattle from the Canadian birth herd of the index cow. These cattle were mentioned by Dr. Brian Evans, Chief Veterinary Officer for Canada, in the Jan. 6, 2004, technical briefing. These heifers are not part of the original 81 animals and it is not known how many of the 17 actually entered the United States. To date, six animals have been identified in the United States:

- 3 were at a facility in Quincy, WA.
- 1 was at a facility in Boardman, OR.
- 1 is at a facility in Othello, WA.
- 1 is at a facility in Burley, ID.

Trade Issues

Specific trade information can be found at
http://www.aphis.usda.gov/lpa/issues/bse/bse_trade_ban_status.html.

Other Issues

On Jan. 27, 2004, Secretary Ann M. Veneman testified before the Senate Committee on Agriculture, Nutrition and Forestry. Text of her testimony is available at
<http://www.usda.gov/Newsroom/0042.04.html>.

Additional information on BSE can be obtained by visiting the USDA website at
<http://www.usda.gov/BSE>. Past BSE updates can also be found at
<http://www.aphis.usda.gov>.