Annual ADFSL Conference on Digital Forensics, Security and Law 2015

May 20th, 9:00 AM

A Review of Recent Case Law Related to Digital Forensics: The Current Issues

Kelly A. Cole
Department of Computer and Information Technology, Purdue University, colek@purdue.edu

Shruti Gupta
Department of Computer and Information Technology, Purdue University, gupta63@purdue.edu

Dheeraj Gurugubelli
Department of Computer and Information Technology, Purdue University, dgurugub@purdue.edu

Marcus K. Rogers
Department of Computer and Information Technology, Purdue University, rogersmk@purdue.edu

A REVIEW OF RECENT CASE LAW RELATED TO DIGITAL FORENSICS: THE CURRENT ISSUES

Kelly Anne Cole, Shruti Gupta, Dheeraj Gurugubelli and Marcus K Rogers
Department of Computer and Information Technology
Purdue University
West Lafayette, IN 47907
colek@purdue.edu, gupta63@purdue.edu, dgurugub@purdue.edu and rogersmk@purdue.edu

ABSTRACT

Digital forensics is a new field without established models of investigation. This study uses thematic analysis to explore the different issues seen in the prosecution of digital forensic investigations. The study looks at 100 cases from different federal appellate courts to analyze the cause of the appeal. The issues are categorized into one of four categories, 'search and seizure', 'data analysis', 'presentation' and 'legal issues'. The majority of the cases reviewed related to the search and seizure activity.

Keywords: Computer Investigation, Case Law, Digital Forensics, Legal Issues, and Courts

1. INTRODUCTION

Digital forensics (DF) is still in its infancy, resulting in rapid growth and formation. Legal concerns surrounding this field must soon be addressed in order for it to function fittingly as a scientific field. Several dominating legal issues relevant to DF have come to light including lack of standards and certifications, analysis and preservation concerns and admissibility of evidence issues (Meyers & Rogers, 2004). For this paper, the issues in appellate court proceedings surrounding the digital forensics field are examined and more fully addressed. But first what is digital evidence?

The DoJ (2008) describes digital evidence as, "information and data of value to an investigation that is stored on, received, or transmitted by an electronic device. This evidence is acquired when data or electronic devices are seized and secured for examination" (pg.1). For example, illegal photos, chats, log files and emails are examples of potential digital evidence used in the courts. Who relies on digital forensic evidence and research related to cyber crimes?

Academia, law enforcement, the military, the private sector and the legal system all rely on digital forensic evidence and research related to cyber crimes as they are all using and or interpreting the same technologies (Palmer, 2002). Differences exist among how each of these disciplines put digital forensics into practice. Investigators in law enforcement (LE) conducting investigations in search of electronic evidence useful for a prosecution must follow the exact guidelines set by the court. The primary objective for the private sector is to maintain business continuity in the face of an incident. Thus, the goal of the digital investigation is recovery from the incident, in real time, and prosecution goals (if any) are secondary.

The military acquires digital evidence in the same way that businesses do except that their objectives are more focused on the protection of highly confidential digital data (Palmer, 2002). They all look to digital forensic research in order to formulate best practices when using digital technology and they also look to the courts for protection and retribution against malicious attacks. Currently the courts are facing rather tough questions from the fairly new digital world.

Smith and Kenneally (2008) ask the question of how do we prevent previous case law decisions from overlooking new issues or disregarding more complex ones. For instance they proposed the question, "should an e-mail or log be denied admissibility because it was retrieved from a database that was unsecured and

subject to tampering" ? Information technology experts are frequently called upon to objectively answer such data integrity questions for the court. Currently the bar for proving reliability and authenticity of digital evidence is not very high (Smith & Kenneally, 2008). Typically, evidence will be admitted if the testifying witness had firsthand knowledge of the evidence, if the evidence is a product of an automated process or system, or the digital record(s) meet the business records exception to the Hearsay Rule. Thus, data tampering is considered unlikely by the courts (Smith & Kenneally, 2008). As courts become more familiarized with digital evidence vulnerabilities, they will start scrutinizing the trustworthiness of evidence from computer systems and investigative methods (Chaikin, 2007). Over time the courts will also better apply constitutional amendments to the digital world.

There is still ambiguity about the interpretation of the 4th Amendment protections to the digital world (Nance & Ryan, 2011). In regards to the 4th Amendment and digital evidence searches, the plain view exception and the closed container rule has brought up significant attention. When an investigator is conducting a search within the scope of a warrant and comes across contraband in plain view, the officer is allowed to seize it. The issue with digital evidence is that the scope is sometimes overbroad. With a valid warrant the investigator can search the whole hard drive as if it were a container, thus all of its contents are in plain view. Depending on the judge and evidence submitted, courts may limit the scope of such searches (Trepel, 2007).

Stahl et al., (2012) claim that lawyers, computer experts, legislators and judges do not share the same knowledge and understanding of computer technologies that is needed in order to address the conflicts between forensic technology and law. The following section provides the related work surrounding legal issues in the computer forensics field, followed by the methods, results, limitations and our conclusion.

2. RELEVANT LITERATURE

Meyers and Rogers (2004) discussed that search and seizure methods are disputed most often in regards to digital forensic investigations and that improper search and seizure methodology (missing steps) used during the digital investigation could potentially impact in the inadmissibility of the evidence. The current research investigates if this is true over the past 10 years and which steps are missed most often.

Shinder (2003) addresses the legal issues in a similar manner as the present paper. She identifies the various issues and discusses the case law that highlights those issues. However, she restricts her discussion mostly to an in-depth analysis of the issues related to search and seizure. This paper looks at all the issues that arise within the dataset of cases. Also, Shinder (2003) looks at milestone cases instead of examining "random" cases like the present study.

Meyers and Rogers (2004) presented an overview of the issues faced in the field on computer forensics. They highlighted the lack of standardization as the biggest issues but also explain the legal hurdles related to search and seizure and expert qualifications. Brungs and Jameison (2005) conducted research to identify and classify the main legal issues associated with digital forensics. Conducting the research in Australia, they recruited eleven experts to discuss and identify the legal issues related to computer forensics. They then ranked the issues and provided a classification scheme for the various legal issues.

Wegman (2006) discusses the various issues related to the admissibility of evidence in the court of law. He outlines the main laws related to computer forensic investigation and highlights the difficulties in interpreting the usual criminal laws to digital investigations. He provides more of an overview of the legal aspects. Liles et al. (2009) furthered the research by Brungs and Jameison (2005) but conducting a similar survey but in the United States. They increased the survey size to sixty-nine respondents and performed a comparative analysis of the results with those of Brungs and Jameison.

Greiman and Chitkushev (2010) deal with the legal aspects of computer forensics from an academic perspective. They delve into the ramifications of understanding the legal framework for digital investigations. They attempt to design an academic curriculum to effectively

address legal concepts like cyber-law, jurisdiction issues etc.

3. METHODS

The appellate cases were randomly selected using the FindLaw database and through using the keywords 'computers', 'computer', 'online', 'digital', 'computer crime', 'digital evidence', and 'computer investigations'. The researchers examined 100 appellate court cases from all districts related to digital forensic investigations within the past 10 years, in search of the most profound issues during digital investigations (see Appendix A for a list of reviewed cases).

The thematic analysis method was used (Braun & Clarke, 2006). Thematic analysis involves the searching across a dataset to find repeated patterns of meaning (Braun & Clarke, 2006). The researchers took an inductive data analysis approach. An inductive approach means the themes identified are strongly linked to the data themselves and are not fit to a pre-existing coding frame (Patton, 1990). The researchers read and re-read the cases many times, and used open coding of the data until major themes related emerged. 87 cases fell into 4 themes. The 4 themes presented next, offer valuable insights into the issues taking place in courts surrounding digital technologies (see figure 1).

4. RESULTS

Overall, 24 of the cases were reversed and the rest of the cases were upheld in favor of the prosecutor. Four major themes emerged from the data:

4.1 Search and Seizure

Among the 100 cases that the researchers examined, 41 of the appeals deal with issues during the collection phase of the digital forensic process. The issue most dealt with by the court was exceeding the scope of the warrant (15), followed by the defendants claim to an expectation of privacy which includes warrantless searches (9), followed by the claim that standards for probable cause were not met (7), followed by the claim that consent to search was not given (5) and lastly, staleness or invalid warrant (5). Our findings are consistent with the research of Meyers and Rogers (2004) who suggested that search and seizure methods would be disputed most often in regards to digital forensic investigations. Improper search and seizure methodology (missing steps) used during the digital investigations results in the inadmissibility of the evidence (Meyers & Rogers, 2004).

4.2 Data Analysis

Among the 100 cases that the researchers examined 10 fell into the data analysis theme. The issues dealt with the most were errors in a programs' output or a program not working correctly (4), unreliability of time stamps and mac times (3), computer was wiped or contaminated during examination (3).

4.3 Presentation Issues

Among the 100 cases that the researchers examined, 5 of the appeals fell into the presentation and expert witness theme. The issue most dealt with by the courts was the failure to preserve text messages or images for presentation (3), followed by whether or not an expert witness must fully understand the source code of a tool or how it works (2).

4.4 Legal Issues

Among the 100 cases that the researchers examined, 31 fell into the legal theme. A popular issue dealt with by the court was whether or not an image of an abused child was real, virtual, or computer generated (6). Followed by the defendants refusal to decrypt passwords or files (1), unauthorized access or whether one had access or not to specific files (6), sentencing issues which includes double counting and sentence enhancement issues (13) and lastly, knowing possession (4). The four major themes that have emerged revealed the major issues being brought up by the courts.

Figure 1 Theme Frequencies

Search and Seizure	**Affirmed**	**Reversed**
Exceeding the scope of the warrant	15	4
Expectations of privacy/warrantless search	9	2
Standards for probable cause were not met	7	2
Consent to search was not given	5	1
Staleness or invalid warrant	5	1
Total	**41**	**10**
Data Analysis	**Affirmed**	**Reversed**
Errors in a programs' output or a program not working correctly	4	
Unreliability of time stamps and mac times	3	1
Computer was wiped or contaminated during examination	3	1
Total	**10**	**2**
Presentation and Expert Witness	**Affirmed**	**Reversed**
Failure to preserve text messages or images for presentation	3	1
Must an expert witness fully understand the source code of a tool or how it works	2	
Total	**5**	**1**
Legal Issues	**Affirmed**	**Reversed**
Whether or not an image of an abused child was real, virtual, or computer generated	6	1

The defendants refusal to decrypt passwords or files or pleading the 5th	2	1
Unauthorized access or whether one had access or not to specific files	6	2
Sentencing issues which includes double counting	13	6
Knowing possession	4	1
Total	**31**	**11**
Overall Total	**87**	**24**

4. CONCLUSION

This study consisted of a small sample size. While it would be difficult to make generalizations about the nature of prosecution issues in digital forensics investigations, the study gives us a good glimpse into a subset of problems that are experienced.

One major opportunity for knowing the issues that are being brought up in the courts surrounding digital evidence is awareness for law enforcement. Now that we are aware of the specific search and seizure issues we can better educate police officers in that area of computer investigation. The study showed that 24 of the cases had their decisions reversed in the appellate court. This is a concern for the digital forensics community.

The study also reaffirms that search and seizure procedures need to be carefully adapted to work within the digital realm. The largest issue seen was ambiguity in the scope of the warrant. There were also issues where law-enforcement officers did not stop the search when encountered with new information and apply for another warrant. Another warrant related issue seen was that the warrant was not specific enough. For most of these cases, the court ruled in good faith but this could change as courts become more strict regarding the scope of the warrant. In general, law enforcement officers need specific training in search and seizure procedures for digital evidence. Another issue observed was related to defendant claims that the tool was not functioning properly. The reliability of tools is often discussed as an area of concern, with most of the tools used not subject to scientific testing. The real authenticity of digital images was also questioned in court. With child pornography being a major cyber crime to contend with, ways to prove the "realness" of an image will be important.

This study is limited to 100 cases within the last 10 years. The cases were randomly selected using the FindLaw database and through using the keywords 'computers', 'computer', 'online', 'digital', 'computer crime', 'digital evidence', and 'computer investigations'. The researchers could not get access to police reports therefore some of the issues may have not been brought up in the appellate court briefs.

As mentioned earlier, the study employed a small sample size, which makes it difficult to generalize the results. However, the trend seen among the 100 cases is consistent with the discussion in the digital forensic community about the nature of the issues seen. With attention drawn to these issues, it might be possible to speedup the prosecution of cases and lower the rate at which cases are appealed. Future work in this area should target a much bigger sample size and perform a more detailed analysis of the issues seen.

REFERENCES

[1] Braun, V. and Clarke, V. (2006). Using Thematic Analysis in Psychology. Qualitative Research in Psychology, 3 (77-101).

[2] Beebe, N. (2009). Digital forensic research: The good, the bad and the unaddressed. In *G.* Peterson and S. Shenoi (Eds.), *Advances in digital forensics* (pp. 17-36). IFIP International Federation for Information Processing. Boston.

[3] Brungs, A., & Jamieson, R. (2005). Identification of legal issues for computer forensics. *Information Systems Management; 22*(2), 57-67.

[4] Chaikin, D. (2007) Network investigations of cyber attacks: the limits of digital evidence *Crime Law Social Change, 46*, 239–256 doi: 10.1007/s10611-007-9058-4.

[5] Daubert v. Merrel Dow Pharmaceuticals, Inc., (1993) 509 U.S. 579.

[6] Kuhmo Tire v. Carmichael, (1998) 119 S.Ct. 37, 142 L.Ed.2d 29, 69 USLW 3228

[7] DoJ (2001). *Electronic crime scene investigation: a guide for first responders*. U.S. Department of Justice, 1-74. Retrieved from https://www.ncjrs.gov/txtfiles1/nij/187736.txt.

[8[Greiman, V., & Chitkushev, L. (2010). Legal frameworks to confront cybercrime: a global academic perspective. *5th Internation Conference on Information Warfare and Security.*

[9] Jerry Wegman. (2005). Computer forensics: Admissibility of evidence in criminal cases. *Journal of Legal, Ethical and Regulatory Issues, 8*(1).

[10] Liles, S., Rogers, M., & Hoebich, M. (2009). A survey of the legal issues facing digital forensic experts. *Advances in Digital Forensics V*, (267–276).

[11] Maxwell, J. (2005). Qualitative Research Design: an interactive approach. 2nd edition. Sage publications, 41.

[12] Meyers, M., & Rogers, M. (2004). Computer forensics: The need for standardization and certification. *International Journal of Digital Evidence, 3*(2).

[13] Nance, K., & Ryan, D. J. (2011, January). Legal aspects of digital forensics: a research agenda. In *System Sciences (HICSS), 2011 44th Hawaii International Conference on* (pp. 1-6). IEEE.

[14] Palmer, G. (2002). Forensic analysis in the digital world. *International Journal of Digital Evidence, 1*, 1-6.

[15] Shinder, D. L. (2003, December). Understanding legal issues. *Law & Order, 51*(12), 38-42.

[16] Smith, C.F. & Kenneally, E.E. (2008). Electronic Evidence and Digital Forensics Testimony in Court. Handbook of Digital and Multimedia Forensic Evidence. Ed.Barbara, J. © Humana Press Inc., Totowa: NJ. (8), 103-132.

[17] Stahl, B., Carroll-Mayer, M., Elizondo, D., Wakunma, K., & Zheng, Y. (2012). Intelligence Techniques in Computer Security and Forensics: at the boundaries of ethics and law. *Computational Intelligence for Privacy and Security, 394*, 237-258.

[18] Trepel, Samantha (2007).Digital Searches, General Warrants, and the case for the Courts. *Yale J.L. & Tech.* 120, 1-45.

APPENDIX A REVIEWED CASES

1. U.S. v Habershaw Criminal No. 01-10195-PBS, 2002 U.S. Dist. Lexis 8977.
2. Williford v. Texas. (2004).127 S.W.3d 309; Tex. App.

3. Taylor v. Texas, 02-11-00092-CR
4. Ohio v. Brian Cook. (2002). 149 Ohio App. 3d 422; 429

5. U.S. v. Marinko, No. 09-30430 (9th Cir. 10-22-2010)

6. Ohio v. Anderson. (2004). Case No. 03CA3 3-02-0415

7. Four Seasons Hotels and Resorts v. Consorcio Barr, 320 F.3d 1205 (11th Cir. 2003).

8. Melendez-Diaz v. Massachusetts, 07-591 (Supreme Court June 25, 2009).

9. U.S. v. Rosa, 09-0636-cr (2nd Cir. 10-27-2010)

10. U.S. v. Dye, No. 09-3410 (3rd Cir. 10-22-2010)

11. U.S. v. Merz, No. 09-3692 (3rd Cir. 10-12-2010)

12. U.S. v. Dennington, No. 10-1357 (3rd Cir. 10-7-2010)

13. U.S. v. Jean-Claude, 09-5138 (10th Cir. 10-29-2010)

14. U.S. v. Suarez, Criminal Action No.: 09-932 (JLL) (N.J. 10-21-2010)

15. U.S. v. Christie, No. 09-2908 (3rd Cir. 9-15-2010)

16. In Matter of the Application of U.S., No. 08-4227 (3rd Cir. 9-7-2010)

17. U.S. v. Comprehensive Drug Testing, Nos. 05-10067, 05-15006, 05-55354 (9th Cir. 9-13-2010)

18. U.S. v. Williams, No. 10-10426 Non-Argument Calendar (11th Cir. 9-22-2010)

19. U.S. v. Norman, CASE NO. 2:09-CR-118-WKW [WO] (M.D.Ala. 9-24-2010) expectation of privacy for p2p

20. Maggette v. BL Development Corp., NO. 2:07CV181-M-A LEAD CASE, NO. 2:07CV182-M-A (N.D.Miss. 9-2-2010

21. United States v. Highbarger, No. 09-1483, United States Court of Appeals for the Third Circuit, 380 Fed. Appx. 127; 2010 U.S. App. LEXIS 9963, May 6, 2010

22. United States v. Giberson, 527 F.3d 882, 889-90 (9th Cir. 2008)

23. United States v. Hill, 459 F.3d 966, 977-78 (9th Cir. 2006).

24. United States v. Carey, 172 F.3d 1268 (10th Cir. 1999)

25. United States v. Grant, 490 F.3d 627, 633-34 (8th Cir. 2007)

26. US v. Stanley,United States Ninth Circuit 08/02/11 10-50206

27. People v. Stipo, B218512 (05/16/11)

28. ED* US v. Nosal, 10-10038, ninth circuit 04/28/2011

29. US v. Rodriguez, 09-15265 US eleveth circuit 12/27/2010

30. US v. Koch, 10-1789 US Eighth Circuit 11/16/2010

31. US v. Allen, 09-50283 US fifth circuit 11/05/2010

32. US v. Payton, 07-10567 US 9th circuit Decided 07/21/2009

33. *US v. Christie*, No. 09-2908 (3d Cir. Sept. 15, 2010).

34. *US v. Ellyson*, 326 F.3d 522 (4th Cir. 2003).

35. *State v. Grenning*, 174 P.3d 706, 142 Wash. App. 518 (Ct. App. 2008).

36. *United States v. Doe*, 556 F.2d 391 (6th Cir. 1977).

37. *US v. Evers*, 669 F.3d 645 (6th Cir. 2012).

38. *US v. FREERKSEN*, No. 11-6044 (10th Cir. Jan. 24, 2012).

39. *US v. Vadnais*, 667 F.3d 1206 (11th Cir. 2012).

40. *US v. Moreland*, 665 F.3d 137 (5th Cir. 2011).

41. United States v. Lynn, No. 09-10242

42. United States v. Hardy, No. 10-4104, UNITED STATES COURT OF APPEALS FOR THE THIRD CIRCUIT, 2011 U.S

43. UNITED STATES OF AMERICA, Plaintiff - Appellee v. DANIEL JAMES BROUSSARD, Defendant – Appellant No. 11-30274 UNITED

STATES COURT OF APPEALS FOR THE FIFTH CIRCUIT 2012 U.S. App. LEXIS 1876 February 1, 2012, Filed

44. UNITED STATES OF AMERICA, Plaintiff-Appellee, v. OVELL EVERS, SR., Defendant-Appellant. No. 08-5774 UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT 12a0042p.06; 2012 U.S. App. LEXIS 2641; 2012 FED App. 0042P (6th Cir.)

July 28, 2011, Argued

February 10, 2012, Decided

February 10, 2012, Filed

45. UNITED STATES v. BERK

UNITED STATES of America, Appellee, v. Michael A. BERK, Defendant, Appellant. No. 09–2472. July 27, 2011

46. UNITED STATES v. PERAZZA MERCADO

UNITED STATES of America, Appellee, v. José Angel PERAZZA–MERCADO, Defendant, Appellant. No. 07–1511. January 21, 2009

47. UNITED STATES v. LaFORTUNE

UNITED STATES of America, Appellee, v. Girard LaFORTUNE, Defendant, Appellant. No. 06-1699. March 18, 2008

48. UNITED STATES of America, Appellee, v. David RODRIGUEZ-PACHECO, Defendant, Appellant. No. 05-1815. February 05, 2007

49. *US v. Goldsmith*, 432 F. Supp. 2d 161 (D. Mass. 2006).

50. UNITED STATES v. COUNCILMAN

UNITED STATES of America, Appellant, v. Bradford C. COUNCILMAN, Defendant, Appellee. No. 03-1383. August 11, 2005

51. People v. Nazary (2011)191 Cal.App.4th 727 , -- Cal.Rptr.3d –

52. People v. Hawkins (2002) 98 Cal.App.4th 1428 , 121 Cal.Rptr.2d 627

53. UNITED STATES of America, Plaintiff–Appellant, v. David NOSAL, Defendant–Appellee. (2011)

54. UNITED STATES of America, Plaintiff-Appellee, v. Luis Miguel DIAZ-LOPEZ, Defendant-Appellant.

55. UNITED STATES v. HILTON UNITED STATES of America, Respondent, Appellant, v. David HILTON, Petitioner, Appellee. No. 03-1741. April 02, 2004

56. UNITED STATES v. ROBINSON

UNITED STATES of America, Appellee, v. Robert ROBINSON, Defendant, Appellant. No. 03-1403. March 02, 2004

57. US v. Richardson 09-4072 June 11, 2010

58. UNITED STATES v. KING

UNITED STATES of America, v. Richard D. KING, Jr., Appellant. No. 09-1861.

Argued Oct. 27, 2009. -- April 30, 2010

59. UNITED STATES v. TENUTO UNITED STATES of America, Plaintiff-Appellee, v. Vincent J. TENUTO, Defendant-Appellant. No. 09-2075. Argued Nov. 12, 2009. -- February 03, 2010

60. UNITED STATES v. KAIN UNITED STATES of America, Plaintiff-Appellee, v. Andrew Charles KAIN, Defendant-Appellant. No. 08-3396.

61. UNITED STATES v. LAY UNITED STATES of America, Plaintiff-Appellee, v. Dennis LAY, Defendant-Appellant. No. 07-4062. Argued: Jan. 16, 2009. -- October 13, 2009

62. LVRC HOLDINGS LLC v. BREKKA

LVRC HOLDINGS LLC, Plaintiff-Appellant, v. Christopher BREKKA; Employee Business Solutions Inc.; Carolyn Quain; Stuart Smith; Brad Greenstein; Frank Szabo, Defendants-Appellees. No. 07-17116.

Argued and Submitted March 13, 2009. -- September 15, 2009

63. UNITED STATES v. STULTS UNITED STATES of America, Appellee, v. Harold STULTS, Appellant. No. 08-3183. August 14, 2009

64. UNITED STATES v. ROMM UNITED STATES of America, Plaintiff-Appellee, v. Stuart ROMM, Defendant-Appellant. No. 04-10648.

Argued and Submitted Dec. 5, 2005. -- July 24, 2006

65. *United States v. Otero*, CRIMINAL NO. 1: CR-96-005-03 (M.D. Pa. Oct. 31, 2005).

66. UNITED STATES v. ALBERTSON UNITED STATES of America v. Randy A. ALBERTSON, Appellant. No. 09–1049. Argued Sept. 23, 2010. -- May 04, 2011

67. SNYDER v. BLUE MOUNTAIN SCHOOL DISTRICT J.S., a minor, through her parents; Terry SNYDER; Steven Snyder, Appellants v. BLUE MOUNTAIN SCHOOL DISTRICT; Joyce Romberger; James McGonigle. No. 08–4138. Argued June 2, 2009. -- June 13, 2011

68. *US v. Cioni*, 649 F.3d 276 (4th Cir. 2011).

69. *US v. Mann*, 592 F.3d 779 (7th Cir. 2010).

70. *US v. Voelker*, 489 F.3d 139 (3d Cir. 2007).

71. *US v. Trotter*, 478 F.3d 918 (8th Cir. 2007).

72. *US v. Schaffer*, 586 F.3d 414 (6th Cir. 2009).

73. *US v. Mutschelknaus*, 592 F.3d 826 (8th Cir. 2010).

74. *US v. Tenuto*, 593 F.3d 695 (7th Cir. 2010).

75. *US v. John*, 597 F.3d 263 (5th Cir. 2010).

76. *US v. Lewis*, 594 F.3d 1270 (10th Cir. 2010).

77. *US v. Batti*, 631 F.3d 371 (6th Cir. 2011).

78. *US v. Quinzon*, 643 F.3d 1266 (9th Cir. 2011).

79. *US v. Felix*, 561 F.3d 1036 (9th Cir. 2009).

80. *US v. Luken*, 560 F.3d 741 (8th Cir. 2009).

81. *US v. Mitchell*, 365 F.3d 215 (3d Cir. 2004).

82. *US v. Lewis*, 594 F.3d 1270 (10th Cir. 2010).

83. *US v. Patterson*, 576 F.3d 431 (7th Cir. 2009).

84. *US v. Nichols*, 512 F.3d 789 (6th Cir. 2008).

85. *US v. Payton*, 573 F.3d 859 (9th Cir. 2009).

86. *US v. Griesbach*, 540 F.3d 654 (7th Cir. 2008).

87. *US v. GIBERSON*, 527 F.3d 882 (9th Cir. 2008).

88. *US v. Hansel*, 524 F.3d 841 (8th Cir. 2008).

89. *US v. Griffin*, 150 F.3d 778 (7th Cir. 1998).

90. People v. Hertzig, C053674

91. *US v. McCoy*, 323 F.3d 1114 (9th Cir. 2003).

92. UNITED STATES OF AMERICA, Plaintiff-Appellee, United States Court of Appeals Tenth Circuit August 24, 2007 RAY ANDRUS, v. No. 06-3094

93. Coburn v. PN II, Inc., 2:07-cv-00662-KJD-LRL (Nev. 9-30-2010)

94. USA v SLANINA 5th circuit No. 00-20926 Feb 21 2002

95. *Paroline v. US*, 134 S. Ct. 1710, 572 U.S., 188 L. Ed. 2d 714 (2014).

96. United States of America, Plaintiff-Appellee, v. David Daniel Anderson, 7th circuit. Argued November 27, 2001--Decided February 12, 2002.No. 01-1368

97. United States Court of Appeals,Tenth Circuit.UNITED STATES of America, Plaintiff–Appellee, v. Jory Michael NANCE, Defendant–Appellant.No. 13–6188.Decided: September 23, 2014

98. United States Court of Appeals,Tenth Circuit.UNITED STATES of America, Plaintiff–Appellee, v. Gustave Wilhelm BRUNE, Defendant–Appellant. No. 12–3322. Decided: September 19, 2014

99. United States Court of Appeals,Tenth Circuit. UNITED STATES of America, Plaintiff–Appellee, v. John Edward MULLIKIN, Defendant–Appellant. No. 13–1290. Decided: July 15, 2014

100. United States Court of Appeals,Tenth Circuit. UNITED STATES of America, Plaintiff–Appellee, v. Lawrence L. LUCERO, Defendant–Appellant. No. 13–2084. Decided: May 2, 2014

